TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

VERKONHALLINTA TUTKIMUSVERKOSSA

Verkonhallintajärjestelmä Nagios

Esa Lempinen

Tietojenkäsittelyn koulutusohjelma
marraskuu 2006
Työn ohjaaja: Paula Hietala

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t) Esa Lempinen

Koulutusohjelma(t) Tietojenkäsittely

Opinnäytetyön nimi Verkonhallinta tutkimusverkossa. Verkonhallintajärjestelmä Nagios

Työn valmistumis-kuukausi ja -vuosi marraskuu 2006

Työn ohjaaja Paula Hietala **Sivumäärä:** 46

TIIVISTELMÄ

Sähköiset palvelut ja järjestelmät ovat yleistyneet ja tulleet osaksi jokapäiväistä elämäämme. Tietoverkkoja laajennettaessa ja yhdistettäessä 1970-luvulla alettiin kehittää verkonhallinnan teorioita niiden ylläpidon helpottamiseksi. Sittemmin teorioiden pohjalta kehitettiin verkonhallintajärjestelmiä, jotka ovat tänä päivänä kriittinen osa mitä tahansa tieto- ja telekommunikaatioverkkoa.

Tämä opinnäytetyö on tehty toimeksiantona Tampereen ammattikorkeakoululle. Tavoitteena oli tutkia, miten tietoverkkopalveluiden suuntautumisvaihtoehdon hallinnoiman WPK-verkon palvelinten ja palveluiden tilasta ja toimivuudesta voitaisiin saada entistä parempi käsitys. Aiemmin seurantaa ei ollut millään tavalla järjestelmällisesti toteutettu.

Teoriaosuudessa aiheina ovat verkonhallinta, verkonhallinnan osa-alueet ja verkonhallintajärjestelmät. Lisäksi käsitellään verkonhallinnan standardoituja protokollia, jotka ovat SNMP ja CMIP.

Käytännön työssä otettiin käyttöön verkonhallintapalvelin ja Nagios-verkonhallintajärjestelmä, joka seuraa verkon tilaa yksityiskohtaisesti. Mahdollisista ongelmista verkonhallintajärjestelmä ilmoittaa ylläpidolle sähköpostitse tai tekstiviestitse. Järjestelmän web-käyttöliittymästä voidaan myös seurata reaaliaikaisesti eri verkkopalveluiden toimivuutta.

Verkonhallintajärjestelmät antavat ylläpidolle tärkeää tietoa verkon tilasta ja mahdollisista ongelmatilanteista. Niiden tärkein tehtävä on helpottaa ylläpidollista rasitetta, jota varsinkin ongelmatilanteissa pääsee kertymään. Lisäarvoa järjestelmä tuo, jos sen tarjoamilla tiedoilla voidaan ennakoida ja perustella tulevaisuudessa tarvittavia hankintoja entistä paremmin.

Johtopäätöksenä voidaan myös todeta, että avoimen lähdekoodin Nagios-verkonhallintajärjestelmä soveltuu hyvin pienten ja keskisuurten verkkojen hallintajärjestelmäksi.

Avainsanat Verkonhallinta SNMP Verkonhallintajärjestelmät Nagios

TAMPERE
POLYTECHNIC

Author(s)	Esa Lempinen
Degree Programme(s)	Business Information Systems
Title	Network Management in a Research Network. Network Management System Nagios
Month and year	November 2006
Supervisor	Paula Hietala **Pages:** 46

ABSTRACT

Electronic services and systems have become common and a part of our everyday lives. As information networks were expanding and being linked up in the 1970s, network management theories were developed in order to ease the administration. Afterwards, these theories were used in creating network management systems, which are nowadays a critical part of any information- or telecommunications network.

This thesis has been commissioned by Tampere Polytechnic. The objective was to examine, how the conception of server's functionality could be improved in WPK-network, which is controlled by the Network Services orientation alternative. Formerly, no systematic monitoring was being carried out.

The topics in the theory section are network management, its objectives and network management systems. In addition, the standard protocols of network management, SNMP and CMIP are covered.

Practical tasks consisted of installing a management server and Nagios network management software, which monitors the state of the network in detail. Any problems would be notified to the administration by email or sms. Also the state of the network and its services could be checked at any time in the web user interface.

Network management systems offer vital information of the state of the networks and possible problems to the administrators. Their main task is to ease the administrative overhead, especially in crisis. The system becomes even more valuable, if its information can be used in order to predict and justify the investments needed in the network.

As a conclusion, the open source Nagios network management system suits well in managing small and mid-sized information networks.

Keywords Network management SNMP Network management systems Nagios

SISÄLLYSLUETTELO

Lyhenteet ja selitykset

CGI (Common Gateway Interface), web-ympäristön tekniikka, jonka avulla selain voi lähettää dataa palvelimella suoritettavalle ohjelmalle. CGI määrittää standardin tähän datan välitykseen.

CMIP (Common Management Information Protocol), OSI-mallin mukainen verkonhallintaprotokolla.

DES (Data Encryption Standard), Yhdysvalloissa liittovaltion standardiksi vuonna 1976 valittu salausmenetelmä, jota on käytetty laajasti ympäri maailmaa. Siitä kehitetyttyjä algoritmejä (kuten 3DES) on edelleen käytössä.

DHCP (Dynamic Host Configuration Protocol), verkkoprotokolla, jonka tärkein tehtävä on jakaa ip-osoitteita verkkoon kytkeytyville laitteille.

DNS (Domain Name System), nimipalvelinjärjestelmä. Tallentaa ja yhdistää monentyyppistä verkkotunnustietoa, tärkeimpänä tehtävänä muuntaa verkkotunnusosoitteet kommunikaation mahdollistaviksi ip-osoitteiksi.

Domain Controller, ohjauspalvelin. Windows-palvelinjärjestelmissä Active Directory –käyttäjätietokannan ja hakemistopalvelun ylläpitäjä. Vastaa esimerkiksi autentikointipyyntöihin (esim. domainiin kirjautuminen, oikeuksien tarkistus). AD mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille.

EGP (Exterior Gateway Protocol), reititysprotokolla jota käytetään autonomisten järjestelmien yhdistämiseen. Nykyään BGP (Border Gateway Protocol) on syrjäyttänyt EGP:n lähes kokonaan.

FCAPS (Fault-management, Configuration, Accounting, Performance, Security), ISO:n määrittelemä malli verkonhallinnalle.

IETF (The Internet Engineering Task Force), Internet-protokollien standardoinnista vastaava organisaatio.

IIS (Internet Information Services), Microsoftin kehittämä palvelinohjelmistokokonaisuus. Maailman toiseksi käytetyin web-palvelinohjelmisto, varsinkin yrityspohjaisissa järjestelmissä.

ISO (International Standards Organization), kansainvälinen standardointiorganisaatio, jonka määrittelemiä standardeja käytetään laajasti.

NAT (Network Address Translation), osoitteenmuunnos. Tekniikka, jolla yksityisiä harmaan sarjan ip-osoitteita käännetään julkisiksi osoitteiksi. NAT:ia hyödyntäen voi yhden julkisen ip-osoitteen takana olla tuhansia koneita.

NRPE (Nagios Remote Plugin Executor), verkonhallintajärjestelmä Nagioksen taustaprosessi valvottaville palvelimille. Käytetään useimmiten sellaisissa tapauksissa, joissa haluttua tietoa ei voida selvittää esimerkiksi SNMP:n avulla, vaan se pitää kysellä palvelimella lokaalisti.

NSCA (Nagios Service Check Acceptor), verkonhallintajärjestelmä Nagioksen lisäosa, jota käytetään tarkistustietojen välittämiseen Nagios-palvelimelta toiselle.

OSI-malli (Open Systems Interconnection Reference Model) kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa, jossa kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs. Kehitetty 1980-luvun alussa. ISO:n kansainvälinen standardi.

Sharepoint (Windows Sharepoint Services), portaalijärjestelmä, johon voidaan liittää sivustoja käyttäjäoikeuksineen esimerkiksi projektiryhmien tiedonvälitystä varten.

SGMP (Simple Gateway Monitoring Protocol), SNMP:n edeltäjä. Tietoliikenneprotokolla, joka on suunniteltu pääasiassa reititinten valvontaan.

SNMP (Simple Network Management Protocol), TCP/IP –verkkojen hallinnassa käytettävä tietoliikenneprotokolla.

TCP (Transmission Control Protocol), tietoliikenneprotokolla, jolla luodaan internet-tietokoneiden välille yhteyksiä. Protokolla pitää huolta siitä, että tavujonot pilkotaan ip-paketeiksi ja että paketit saapuvat perille oikeassa järjestyksessä (luotettava, yhteydellinen).

UDP (User Datagram Protocol), TCP/IP-yhteyskäytäntö, jolla sovellus voi lähettää tietoja toiselle tietokoneelle. Eroaa TCP:stä siten, että paketin perillepääsyä ei vahvisteta ja siten saadaan suurempi nopeus (epäluotettava, yhteydetön).

Verkonhallinta (Network management), tyypillisesti toteutettu laajoissa tietoverkoissa kuten tietoliikenneverkot ja telekommunikaatioverkot. Viittaa verkkojen ylläpitoon ja hallintaan.

Verkonhallintajärjestelmä (Network Management System, NMS), on laitteen ja sovelluksen yhdistelmä, jonka tehtävänä on monitoroida ja hallinnoida verkkoa.

VPN (Virtual Private Networking), on tapa, jolla esimerkiksi kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon. Nykyään VPN-määritelmä on laajennettu koskemaan myös yksittäisten etätyöasemien liittämistä yrityksen verkkoon. Yhteys on salattu.

1 Johdanto

Sähköiset palvelut ja järjestelmät ovat yleistyneet ja niistä on tullut osa jokapäiväistä elämäämme. 1970-luvulta alkaen erilliset lähiverkot alkoivat yhdistyä muodostaen suurempia verkkoja ja lopulta internetin. Tuolloin alettiin kehittää myös verkonhallinnan teorioita suurten verkkojen ylläpitoa helpottamaan. Niiden pohjalta on suunniteltu verkonhallintajärjestelmiä, jotka toimivat kriittisenä osana mitä tahansa nykypäivän tietoliikenne- ja telekommunikaatioverkkoa.

Yrityksillä ei ole varaa siihen, että liiketoiminnan kannalta oleelliset järjestelmät eivät toimi halutusti tai lainkaan. Silti IT:lle varattuja resursseja saatetaan hyvinkin pitää entisellä tasollaan tai jopa leikata niitä, tehokkuuden parantamiseksi. Ylläpitäjät reagoivat päivittäin ongelmiin, jotka aiheutuvat odottamattomista muutoksista järjestelmissä. Verkonhallintajärjestelmät auttavat ylläpitäjiä ennakoimaan ongelmia, ratkaisemaan ne nopeammin ja huolehtimaan paremmin verkon yleisestä toimivuudesta. Lisäksi järjestelmät tuovat kustannussäästöjä yrityksille monellakin tavalla.

Opinnäytetyö on tehty toimeksiantona Tampereen ammattikorkeakoululle, jossa toimin tietoverkkopalveluiden WPK-verkon ylläpitäjänä. Suuntautumisvaihtoehdon vastaava opettaja, diplomi-insinööri Harri Hakonen esitti tehtäväksi palvelinten seurantaa, koska tietämys palvelinten tilasta katsottiin nykyisellään riittämättömäksi. Tavoitteena oli jollain tapaa ottaa haltuun palvelinten resurssien ja käytön seuranta.

Teoriaosuuden alussa selvitetään lyhyesti verkonhallinnan avainkäsitteitä ja osa-alueita. Sen jälkeen käsitellään verkonhallintajärjestelmiä, niiden tehtäviä ja ominaisuuksia, verkonhallintajärjestelmien käyttämiä standardoituja protokollia sekä erilaisia verkonhallintasovelluksia, joista yksi valitaan käytettäväksi tietoverkkopalveluiden WPK-verkossa.

Raportin loppuosassa kuvataan käytännön työtä, joka koostui verkonhallintapalvelimen käyttöönotosta, sekä hallintajärjestelmän ja sen vaatimien komponenttien asennuksesta. Käyttöön otettiin myös tekstiviestihälytysjärjestelmä. Lisäksi osuudessa käsitellään mm. sitä, millaisia tietoja järjestelmä verkosta kerää ja miten se tapahtuu. Myös järjestelmän turvallisuus otetaan huomioon.

Lopuksi järjestelmän toimivuus ja ylläpidollisen roolin merkitys asetetaan puntariin, sekä käydään läpi ongelmakohdat ja mahdolliset parannusehdotukset.

2 Verkonhallinta

Verkonhallintaan liittyvät keskeiset kysymykset ovat:

- ovatko kriittisimmät palvelut aina toimintakunnossa yrityksessä?
- voidaanko ongelmat paikallistaa ja priorisoida sekä määrittää resursseja niiden korjaamiseen – automaattisesti?
- voidaanko ongelmat ja muutokset aina hoitaa ennustettavissa olevalla tavalla, jotta minimoidaan riskit, virheet, kustannukset ja haitta liiketoiminnalle?

Yksinkertaistettuna verkonhallinta tarkoittaa käytännössä verkon ja sen palveluiden ylläpitoa. Verkonhallinnan päämääränä on mm. ennaltaehkäistä ja korjata vikoja, hallita käyttöä, suorituskykyä, toiminnallisia asetuksia ja turvallisuutta.

Verkonhallinnan merkitys on korostunut siitä syystä, että verkko ja siihen liittyvät resurssit ovat tulleet korvaamattomiksi. Ongelmien koittaessa opiskelu saattaa vaikeutua, työt pysähtyä, asioiden hoito estyä jne. Verkot ovat myös kasvaneet ja monimutkaistuneet, ja erilaisten verkkopalveluiden määrä on kasvusuunnassa. Tällaisia palveluita ovat esimerkiksi pankki-, sähköposti-, verkkopeli-, verkkokauppa- tai uutispalvelut, sekä kaikki verkon nettisivut.

Jos kaikki verkonhallinta tehtäisiin manuaalisesti, olisivat siihen vaadittavat resurssit täysin kohtuuttomat. Siksi näihin haasteisiin on kehitetty automatisoituja verkonhallintatyökaluja, jotka auttavat verkkojen, laitteiden ja palveluiden menestyksekkäässä hoidossa.

Tässä luvussa esitellään lyhyesti verkonhallinnan osa-alueet ISO:n FCAPS-mallin mukaisesti. Nimitys tulee mallin osa-alueiden nimistä. FCAPS muodostaa kulmakiven tämän päivän verkonhallinnalle ja toimii myös ohjeistuksena sille, millaisia ominaisuuksia verkonhallintajärjestelmissä tulisi olla.

2.1 Vikojenhallinta (Fault Management)

Verkon toiminnan ylläpitämiseksi on pidettävä huolta, että jokainen laite itsessään ja järjestelmä kokonaisuutena on toimintakunnossa. Vikojenhallintatekniikoita käyttämällä verkon ylläpitäjä voi paikallistaa ja ratkaista ongelmia nopeammin kuin ilman niitä. Kun vikatilanne havaitaan, on:

- paikallistettava ongelma
- eristettävä ongelma
- korjattava ongelma, jos mahdollista

Tyypillisessä tapauksessa käyttäjä kirjautuu muualla sijaitsevaan järjestelmään ja liikenne kulkee monien verkkolaitteiden kautta. Yhteys katkeaa ja käyttäjä

ilmoittaa ongelmasta ylläpidolle. Ylläpito alkaa eristämään ongelmaa. Ensin tulisi päätellä, onko kyse käyttäjän ongelmasta, esimerkiksi kirjoitusvirheestä tai käyttäjän yrityksestä päästä paikkaan, johon hänellä ei ole oikeuksia. Jos käyttäjävirheitä ei löydy, voidaan ryhtyä tarkistamaan mahdollisia ongelman aiheuttavia laitteita yksitellen, aloittaen siitä, joka on lähinnä käyttäjää. Muutamien testien jälkeen vika yleensä löytyy ja se korjataan. Lopuksi ylläpito varmistaa, että kaikki toimii normaalisti. Kaikkeen tähän saattaa kulua huomattavasti aikaa.

Vikojenhallinnan hyödyt ovat varsin konkreettiset. Vikojenhallinnan työkalujen hyödyntäminen jättää enemmän aikaa verkon kehittämiselle, kun ongelmien ratkaisuun sitä kuluu vähemmän. Parhaassa tapauksessa nämä työkalut osoittavat tarkalleen, milloin ongelmia ilmenee ja ilmoittavat niistä välittömästi ylläpitäjälle, joka voi korjata ongelmat jopa ennen kuin käyttäjät huomaavat mitään. (Leinwand 1996: 38)

2.2 Kokoonpanon hallinta (Configuration Management)

Verkkolaitteiden asetukset kontrolloivat tietoverkon toimintaa ja käyttäytymistä. Kokoonpanon hallinta on prosessi, jonka päämääränä on löytää laite, jonka asetuksissa on parannettavaa ja konfiguroida se uudelleen.

Kokoonpanon hallinta parantaa ylläpidon kontrollia verkon laitteiden konfiguroinneista tarjoamalla nopean pääsyn tärkeään konfiguraatiodataan. Tuhansista aktiivilaitteista koostuvan verkon dokumentointi vaatii paljon työtä, jos se tehdään manuaalisesti. Kokoonpanon hallintaan kuuluu myös ajantasainen inventaario verkkokomponenteista. Tällainen inventaario auttaa esimerkiksi päättelemään kuinka monta tietynlaista laitetta verkossa on, tai mitä kaikkia käyttöjärjestelmiä ja niiden versioita on käytössä. Kokoonpanon hallinnan inventaariotoiminnon ei tarvitse olla rajoittunut vain verkkolaitteiden jäljittämiseen. (Leinwand 1996: 57-58)

Yksinkertaisen verkonhallinnan konfigurointityökalun tulisi vähintään tarjota keskustietokanta kaikelle verkkoinformaatiolle, kuten verkko-osoitteet, sarjanumerot, fyysinen sijainti sekä muut laitetiedot. Siinä tulisi olla autodiscovery-ominaisuus, joka kysyy laitteilta olennaiset tiedot. Automaattinen tiedonkeruu on erityisen tärkeää, koska se takaa tiedon ajantasaisuuden. Verkkoinventaariotieto on kuitenkin luottamuksellista. Ulkopuolisten päästessä käsiksi tähän tietoon, verkon turvallisuus heikentyy oleellisesti. (Leinwand 1996: 64)

Kehittyneempi työkalu tarjoaa esimerkiksi käytössä olevien asetusten (running config) helpon vertaamisen laitteeseen talletettuihin asetuksiin. Lisäksi järjestelmän tulisi pitää kirjaa muutoksista ja niiden ajankohdista. Siinä missä yksinkertaisempi työkalu toimisi vain yksisuuntaisesti (luku-operaatiot), voi kehittyneemmällä työkalulla myös suoraan vaihtaa asetuksia verkonhallintaohjelmistosta koskematta itse laitteeseen millään tavalla. (Leinwand 1996: 65)

2.3 Käytönhallinta (Accounting Management)

Käytönhallinta on verkonhallinnan osa-alue, jossa tarkastellaan verkon resurssien käyttöä käyttäjä- ja ryhmätasolla. Näin voidaan varmistaa, että käyttäjillä on varmasti riittävät resurssit. Käytönhallintaan liittyy myös käyttöoikeuksien hallinta. Käytönhallintaan voivat liittyä myös käyttörajoitukset tai käyttäjien laskutus käytettyjen resurssien mukaan. (Leinwand 1996: 125-126)

Käytönhallinta antaa verkon ylläpitäjälle mahdollisuuden mitata ja raportoida käyttötietoa, joka on eritelty esimerkiksi ryhmiin tai yksittäisiin käyttäjiin. Tietoa voidaan käyttää laskutuksessa, resurssien kohdentamisessa tai kustannuksien laskemisessa ryhmäkohtaisesti. Käytönhallinta myös auttaa ymmärtämään verkon käyttöä ja optimoimaan paremmin verkon resursseja. (Leinwand 1996: 126-127)

Koska teknologia kehittyy nopeasti, käytönhallinnan tekniikoita käytetään myös säästöjen hakemiseen vertailemalla erilaisten ratkaisujen hinta-laatusuhdetta. Kun tiedetään paljonko tietoa siirtyy kuukaudessa, voidaan laskea paljonko rahaa kuluu yhden bitin siirtämiseen. Luonnollisesti halutaan siirtää mahdollisimman paljon dataa määritellyn budjetin raameissa. (Leinwand 1996: 128)

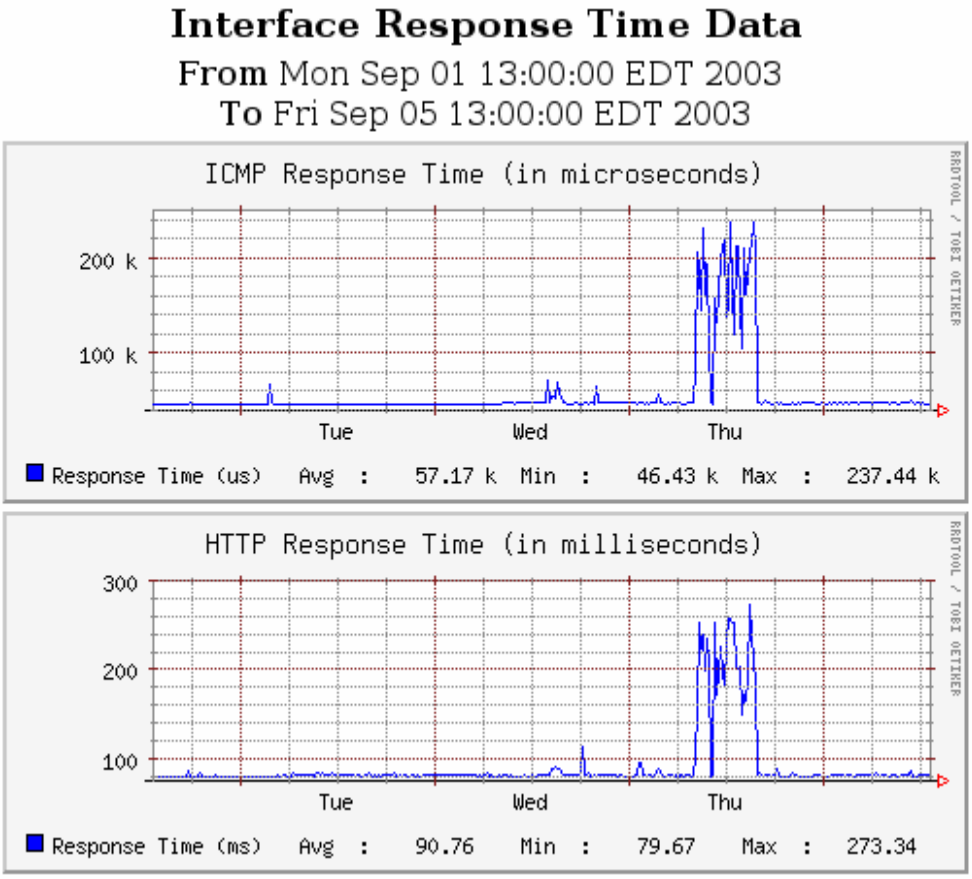
2.4 Suorituskyvyn hallinta (Performance Management)

Tietoliikenneverkko muistuttaa moottoritietä. Siinä missä tie voi tulla ruuhkaiseksi ja näin ollen oleellisesti hidastaa kulkemista, sama voi tapahtua tietoverkoissa. Verkkolaitteet ylikuormittuvat, verkkolinkit saturoituvat, ja lopulta suorituskyky laskee. (Leinwand 1996: 103-104)

Verkko on yhtä hyvä kuin sen heikoin lenkki. Kuormitusta ja suorituskykyä mittaamalla nähdään mitkä laitteet käyvät äärirajoilla. Mitattavia asioita ovat mm. liikennemäärät, käyttöasteet, virheiden määrä ja vasteajat. Suorituskyvyn hallinnan tarjoamilla tiedoilla voidaan varmistaa, että verkon kapasiteetti vastaa käyttäjien tarpeita. Kapasiteetin suunnittelu hyödyttää sekä käyttäjiä että verkon ylläpitäjiä.

Sen lisäksi, että varmistetaan verkon optimaalinen toimintakyky, mittaukset auttavat ennakoimaan mahdolliset ongelmakohdat ja varautumaan tarvittaviin hankintoihin.

Verkonhallintajärjestelmissä yksinkertaiset suorituskyvyn hallintatyökalut antavat tietoa verkon laitteista ja verkkolinkeistä graafisessa muodossa, esimerkiksi histogrammina tai pylväsdiagrammina. Työkalu auttaa löytämään verkon pullonkaulat ja eristämään suorituskykyongelmat. (Leinwand 1996: 111)



Kuva 1: OpenNMS-suorituskykytilastoja (Netstatz Solutions)

Kuva 1 on tyypillinen verkonhallintaohjelmiston tuottama kuvaaja, jossa mitataan laitteelta vasteaikaa ja www-sivupyynnön kuittaamiseen kuluvaa aikaa. Grafiikasta näkee, kuinka verkon suorituskyvyn kanssa on ollut ongelmia eräänä torstai-päivänä. Tilastosta voidaan myös päätellä, että kyse on nimenomaan tiedonsiirron ongelmasta, koska nimenomaan pakettien kulku on hidasta (ICMP response) ja se vaikuttaa kaikkeen liikenteeseen, esimerkiksi kuvan http-liikenteeseen. Tällaisen vian voi aiheuttaa esimerkiksi jokin vikatilanne reitittimessä tai reitittimen ylikuormittuminen suuren liikennemäärän vuoksi.

2.5 Turvallisuudenhallinta (Security Management)

Turvallisuudenhallinnalla tarkoitetaan luottamuksellisen tiedon suojaamista verkkoon liitetyillä laitteilla kontrolloimalla pääsykohtia tuohon tietoon. Luottamuksellinen tieto voi olla mitä tahansa tietoa, jonka organisaatio haluaa suojata, kuten palkkatiedot, asiakastietokannat, tutkimustiedot tai kehityssuunnitelmat. (Leinwand 1996: 75)

Turvallisuudenhallinta antaa ylläpidolle mahdollisuuden suojata tietoa rajoittamalla käyttäjien pääsyä työasemille ja verkkolaitteille. Lisäsuojaa saadaan asettamalla hälytyksiä mahdollisten murtoyritysten tapahtuessa. (Leinwand 1996: 75)

Turvallisuudenhallinnassa verkonhallinnan osa-alueena ei kuitenkaan ole kyse sovellusten tai käyttöjärjestelmien turvallisuudesta, eikä myöskään fyysisestä turvallisuudesta. Ilman näitä verkon turvallisuudenhallinta olisi kuitenkin turhaa, koska suojaukset voitaisiin esim. ohjelmistojen haavoittuvuuksien vuoksi kiertää.

Ehkä yleisin huolenaihe käyttäjän liittäessä koneensa verkkoon on mahdollinen tietoturvauhka. Välttääkseen tämän ongelman, voitaisiin verkkoliikenne estää kokonaan ja siirtää tiedot siirrettävällä medialla, kuten muistitikulla. Näin tietoon pääsisi vain fyysisesti käsiksi. Vaikka tämä metodi on turvallinen, se ei ole erityisen tehokas ja poistaa tehokkaasti verkon käyttötarpeen. Oikein hoidettuna turvallisuudenhallinta tarjoaa käytännöllisemmän vaihtoehdon tiedon turvaamiselle ja lisää käyttäjien luottamusta verkon tietoturvaan. Luottamuksen lisääntyminen ja tiedon turvaaminen ovat turvallisuudenhallinnan kaksi suurinta hyötyä. (Leinwand 1996: 76-77)

3 Verkonhallintajärjestelmät

Verkonhallintajärjestelmä on käytännössä laitteen ja sovelluksen yhdistelmä, jonka tehtävät ovat edellisessä luvussa esitellyn FCAPS-mallin mukaisia, vaikka läheskään kaikki järjestelmät eivät kata koko FCAPS-mallia. Verkonhallintajärjestelmiä on sekä kaupallisia, että vapaan lähdekoodin projekteja.

Verkonhallintajärjestelmät toimivat useimmiten verkon laitteiden ja palveluiden kyselemisellä saadun tiedon varastointipaikkana. Lisäksi ne huolehtivat siitä, että ongelmista lähtee välittömästi tieto verkon ylläpitäjille. Esimerkiksi tavallinen nettiliittymiä tarjoava yritys ei voi odottaa sitä, että asiakkaat valittavat ongelmasta ennen kuin ongelmalle aletaan tehdä jotain. Pitää olla järjestelmä, josta ongelmatilanteet voi aina todeta ja määrittää resursseja niiden korjaamiseen.

Verkonhallintajärjestelmät kyselevät tietoja verkon aktiivilaitteilta monin eri tavoin. Kaksisuuntaiseen keskusteluun tarvitaan kuitenkin verkonhallintaprotokollia. Verkonhallintaprotokollat ovat standardoituja verkonhallinnan komponentteja.

3.1 Verkonhallintaprotokollat

Protokolla tarkoittaa kieltä, jolla laitteet keskustelevat. Luonnollisesti molempien laitteiden pitää käyttää keskenään samaa protokollaa, jotta tiedonvaihto on mahdollista. Verkonhallinnassa kommunikoivat laitteet ovat pääasiassa verkonhallintaohjelmisto ja hallinnoitava laite.

On kahdenlaista yhteydenpitoa. Yleisempi on se, jossa hallintajärjestelmä pyytää tietyin väliajoin jotain tietoa laitteelta, esimerkiksi prosessorin käyttöastetta tai käyttäjien määrää http-palvelimella. Mutta joissain tapauksissa on myös mahdollista suorittaa konfigurointitoimenpiteitä laitteille. Esimerkiksi monia Ciscon ja HP:n verkkolaitteita, erityisesti järeämpiä yrityskäyttöön tarkoitettuja, voi konfiguroida SNMP:n avulla.

3.1.1 SNMP

Simple Network Management Protocol luotiin 1980-luvun lopulla, jotta ratkaistaisiin TCP/IP-pohjaisen internetin hallinta. Verkossa oli monenlaisia laitteita, joiden ongelmatilanteiden hoitamiseen tarvittiin yhteinen etähallintamekanismi. ISOn verkkohallintastandardi, CMIS/CMIP oli monimutkainen ja sen kehitystyö vei liikaa aikaa. Päätettiin luoda SGMP:n (Simple Gateway Management Protocol) pohjalta väliaikainen protokolla, jotta OSI-mallipohjaisen CMIPin kehittämiseen saataisiin lisää aikaa ja se voitaisiin ottaa käyttöön myöhemmin. (Drake 1991: 1)

SNMP on sovellustason protokolla, joka helpottaa hallintatiedonvaihtoa verkkolaitteiden välillä. Se on osa TCP/IP protokollapinoa. SNMP antaa mahdollisuuden hallinnoida verkon suorituskykyä, löytää ja ratkaista verkko-ongelmia ja suunnitella verkon laajennuksia keskitetysti. (Cisco 2002: SNMP)

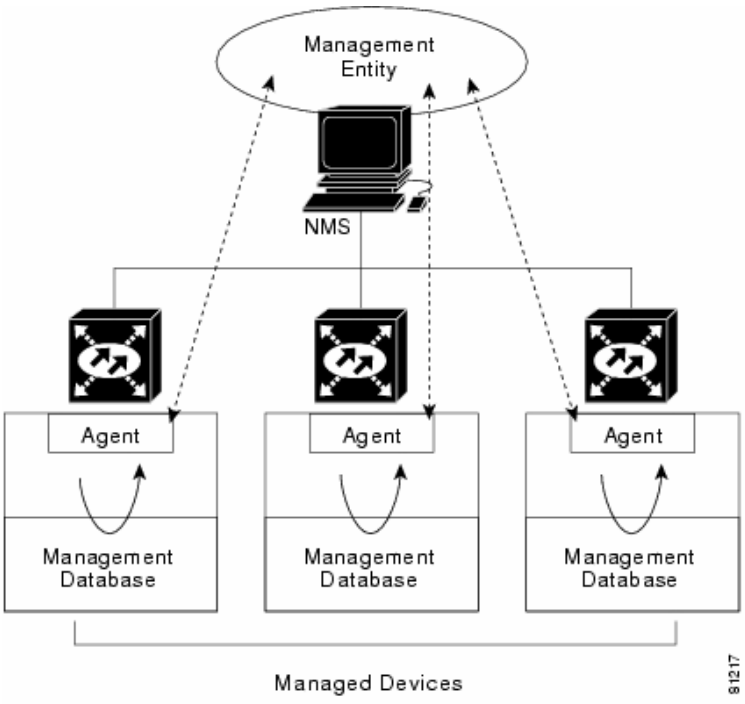
TCP/IP verkonhallinta koostuu kolmesta osasta (Stevens 2000: 359-360)

- Management Information Base (MIB). MIB määrittelee mitä muuttujia verkkoelementit ylläpitävät. MIB on tietokanta, joka sisältää tietoa laitteesta ja sen toiminnasta. Näitä tietoja voidaan kysellä SNMP-protokollalla.

- Structure of Management Information (SMI). SMI määrittelee MIB:n rakenteen ja tunnistusjärjestelmän, jota käytetään viittaamaan MIB-tietokannassa oleviin muuttujiin.

- Simple Network Management Protocol (SNMP). Elementin ja managerin välinen protokolla. RFC 1157:ssä määritelty vaihdettujen pakettien formaatti. Monia kuljetusprotokollia voitaisiin käyttää SNMP:n kanssa, mutta normaalisti käytetään UDP-protokollaa.

Kuvassa 2 on esitelty SNMP:n perustoimintaa. Hallintajärjestelmä (NMS) keskustelee SNMP-agenttien (tai elementtien) kanssa, jotka noutavat tietonsa laitteen MIB-tietokannasta. Laitteet voivat olla esimerkiksi reitittimiä, kytkimiä tai palvelimia.



Kuva 2: Esimerkki SNMP-komponenteista (Cisco 2002: SNMP)

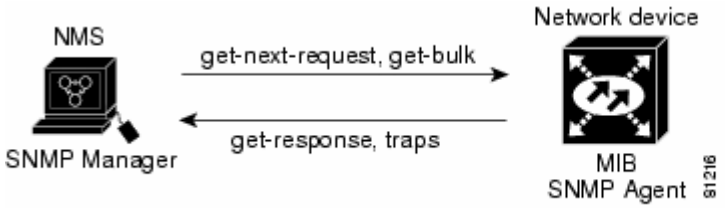
3.1.1.1 SNMP:n perusoperaatiot

Hallinnoituja laitteita kontrolloidaan käyttäen neljäntyyppisiä operaatioita:

- Lukuoperaatiot (read operations), käytetään hallittavien laitteiden valvontaan. Verkonhallintajärjestelmät lukevat laitteiden ylläpitämiä muuttujien arvoja.
- Kirjoitusoperaatiot (write operations), käytetään hallittavien laitteiden ohjaukseen. Verkonhallintajärjestelmät kirjoittavat ja muuttavat laitteiden ylläpitämiä muuttujien arvoja.
- Kauttakulkuoperaatiot (traversal operations), verkonhallintajärjestelmät käyttävät näitä operaatioita määrittämään, mitä muuttujia hallittavat laitteet tukevat.
- Loukut (traps), hallinnoidut laitteet käyttävät loukkuja ilmoittamaan erilaisista tapahtumista, kuten virhetilanteista.

3.1.1.2 Management Information Base

MIB on kokoelma tietoa, joka on järjestetty hierarkkisesti. MIB-tietokantaa käytetään verkonhallintaprotokollalla kuten SNMP:llä (kuva 3). Hallinnoitu objekti (MIB object) on yksi monista hallinnoidun laitteen ominaisuuksista. Hallinnoidut objektit koostuvat yhdestä tai useammasta instanssista, jotka ovat käytännössä muuttujia. (Cisco 2002: SNMP)



Kuva 3: SNMP-agentti keräämässä tietoa MIB:stä (Cisco 2002: SNMP)

Object identifier (OID) yksilöllisesti identifioi hallinnoidun objektin MIB-hierarkiassa. Se on kuin osoite tai puhelinnumero, joka osoittaa oikeaan paikkaan. Esimerkiksi *iso.org.dod.internet.private.enterprise.cisco* viittaa Ciscon MIB-tietueen haaraan, jonka alta löytyy objekteja, jotka sisältävät tietoa Ciscon laitteista. OID voidaan ilmaista myös lyhyemmin numeerisesti, tässä tapauksessa *1.3.6.1.4.1.9*. (Cisco 2002: SNMP)

Hallinnoituja objekteja on kahdenlaisia: skaalautuvia ja taulukollisia. Skaalautuvat objektit määrittelevät yhden objektin, kun taas taulukolliset objektit määrittelevät monia toisiinsa liittyviä objekteja. (Cisco 2002: SNMP)

Yksi helposti ymmärrettävä skaalautuva muuttuja on *tcpCurrEstab*. Se sisältää laitteen senhetkisten avointen tcp-yhteyksien määrän kokonaislukuna.

Taulukollisen muuttujan tapauksessa yhdellä objektilla saattaa olla monta instanssia ja arvoa. Esimerkiksi useamman suorittimen laite palauttaa monta lukua kysyttäessä *CPU loadia* (1.3.6.1.2.1.25.3.3.1.2). Tällaisessa tapauksessa jokainen instanssi saa oman yksilöllisen OID:n, jossa alkuperäisen perään lisätään piste ja lukuja järjestyksessä, jokaiselle instanssille omansa.

MIB 1 määrittelee kahdeksan ryhmää:

- System sisältää yleisiä asetuksia.
- Interfaces sisältää yleistä tietoa muuttujista liitäntätasolla.
- AT (Address Translation) sisältää osoitteenmuunnostietoa.
- Internet Protocol (IP) sisältää tietoa, jolla voidaan seurata IP-kerrosta.
- Internet Control Message Protocol (ICMP) sisältää 26 laskuria, jotka mittaavat tämänkaltaisten vastaanotettujen ja lähetettyjen sekä myös virallisten viestien määrää.
- Transmission Control Protocol (TCP) sisältää tietoa, jolla voidaan seurata TCP:tä käyttäviä sovelluksia.
- User Datagram Protocol (UDP) sisältää tietoa, jolla voidaan seurata UDP:tä käyttäviä sovelluksia.
- Exterior Gateway Protocol (EGP) sisältää tietoa EGP:stä, jos se on käytössä.

MIB 2 lisää kaksi ryhmää listaan:

- Transmission sisältää laitekohtaisia tietoja. On aluksi experimental-kategoriassa, mutta voi päätyä standardiin MIBiin.
- SNMP jonka tiedoilla voidaan seurata SNMP-sovelluksia, sekä esimerkiksi tilastotietoa verkonhallintaliikenteen määrästä.

3.1.1.3 SNMP versio 1

SNMPv1 on alkuperäinen implementaatio SNMP-protokollasta. Se voi liikennöidä TCP/IP-verkkojen lisäksi myös telekommunikaatio-, AppleTalk- ja Novell-verkoissa. AppleTalk ja Novell ovat kuitenkin jo lähes kadonneet ja telekommunikaatiopuolella käytetään yleisemmin CMIP-protokollaa, jota käsitellään luvussa 3.1.2. SNMPv1 käyttää UDP-protokollaa TCP/IP-verkoissa liikennöintiin. SNMPv1 on hyvin laajalti käytetty ja hallitseva verkonhallintaprotokolla internet-ympäristössä. (Cisco 2002: SNMP)

SNMP on yksinkertainen kysely/vastausprotokolla. Verkonhallintajärjestelmä kyselee ja hallinnoidut laitteet palauttavat vastauksia. SNMPv1:ssä on yhteensä vain neljä komentoa, joilla kaikki toteutetaan: Get, GetNext, Set ja Trap. Get-operaatiolla hallintajärjestelmä saa agentilta arvon yhdestä tai useammasta objekti-instanssista. Jos agentti ei pysty palauttamaan arvoa jokaiselle kysellylle objektille, se ei palauta mitään arvoja. GetNext-komennolla kysellään seuraavan objektin arvoa. Agentti käyttää Trap-operaatiota ilmoittaakseen hallin-

tajärjestelmälle jostain erityisestä asiasta, käytännössä ongelmasta. (Cisco 2002: SNMP)

SNMPv1:ssä on määritelty kolmentyyppisiä muuttujien arvoja, joita MIB voi sisältää. Ne ovat kokonaisluvut, oktettijonot ja OID.

3.1.1.4 SNMP versio 2

SNMPv2 on evoluutioversio alkuperäisestä SNMPv1:stä. Teoriassa SNMPv2 tarjoaa monia parannuksia SNMPv1:een, mukaan lukien uudet protokollaoperaatiot. SNMPv2 mahdollistaa myös uudenlaisten tietotyyppien määrittelyn lisäyksenä SNMPv1:n kolmeen tietotyyppiin. Uudet tietotyypit ovat bittijonot, verkko-osoitteet ja laskurit. (Cisco 2002: SNMP)

Uusi pakettityyppi get-bulk-request antaa hallintaohjelmalle mahdollisuuden noutaa suuria määriä tietoa tehokkaasti. Toinen uusi pakettityyppi, inform-request mahdollistaa hallintaohjelmien välisen tiedonvaihdon. Lisäksi SNMPv2 tarjoaa turvallisuuslaajennuksia, perusautentikoinnin ja Community Stringin salauksen. (Stevens 2000: 387)

SNMPv1 ja SNMPv2 eivät ole keskenään yhteensopivia. Niitä voidaan käyttää yhdessä kahdella tavalla: proxy-agenteilla (protokollamuunnin) tai verkonhallintajärjestelmillä, jotka osaavat käyttää kumpaakin protokollaa samanaikaisesti.

3.1.1.5 SNMP versio 3

SNMPv3 on tarkoitettu lähinnä korvaamaan SNMPv2:n puutteet turvallisuudessa ja hallinnoinnissa. SNMPv3:ssa voidaan kaikki viestit salata DES-kryptauksella, mikä ei ollut mielekästä ennen uusia ja tehokkaampia prosessoreita. SNMPv3:n kehittämisessä on käytetty pohjalla SNMPv2 standardidokumentteja. SNMPv3 on edellisistä versioista poiketen kehitetty modulaarisesti, joten sen osia voidaan kehittää erikseen, ilman että koko protokolla muuttuu. (SNMP Research 2006)

Autentikointi SNMPv3:ssa toimii niin, että kaikkien SNMP-tahojen, jotka haluavat kommunikoida, täytyy jakaa salainen autentikointiavain. Tämä avain liitetään lähetettävään SNMPv3-viestiin. Kun vastaanottaja saa viestin, se käyttää samaa avainta uudelleen laskeakseen viestin oikeellisuuden. Näin autentikointimekanismi varmistaa, että saatu viesti on todella lähetetty sieltä mistä viestin otsikkotiedoissa sanotaan. Lisäksi mekanismi takaa sen, että viestiä ei ole muokattu kuljetusvaiheessa ja että sitä ei olla keinotekoisesti viivytetty tai toistettu.

3.1.1.6 SNMP ja turvallisuus

Siitä huolimatta, että SNMP on vahva verkonhallintaprotokolla, SNMPv1:ssä ei ole autentikointimahdollisuuksia ja se on altis monenlaisille turvallisuusongelmille. Ainut SNMP-liikennettä rajoittava tekijä on Community String, eräänlainen salasana, joka pitää olla asetettuna kaikille hallinnoiduille laitteille ja hallintajärjestelmälle samaksi. Ongelmana Community Stringissä on se, että se kulkee salaamattomana SNMP-datagrammissa ja näin ollen se on protokolla-analysaattorilla kaapattavissa verkon liikenteestä. Ulkopuolinen taho voi yrittää suorittaa hallinnointi-operaatioita verkossa esiintymällä oikeutettuna hallinnointitahona. Community Stringin ohella mitä tahansa SNMP-liikennettä voidaan helposti kaapata, tarkastella ja jopa vääristellä (ns. man-in-the-middle attack). Koska SNMPv1 ei tue autentikointia eikä salausta, monet laitevalmistajat eivät implementoi Set-operaatioita laitteisiinsa, alentaen näin SNMP:n monitorointiprotokollaksi. (Cisco 2002: SNMP)

Koska SNMP:tä on kuitenkin tarpeellista käyttää sekä kriittisissä järjestelmissä, että julkisissa verkoissa, SNMPv3 sisältää turvallisuusominaisuuksia. SNMPv3 salaa kaikki tiedonsiirrot ja mahdollistaa vastaajan (yleensä SNMP-agentti) autentikoida käyttäjä, joka on pyynnön takana. SNMPv3 mahdollistaa myös viestin muuttumattomuuden varmistamisen ja pääsylistojen laatimisen, joilla rajoitetaan eri käyttäjien oikeuksia operaatiotasolla. (SNMP Research 2006)

Turvallisuusongelmat eivät kuitenkaan johdu vain protokollasta, vaan myös laitevalmistajien tavasta implementoida SNMP tuotteisiinsa. Esimerkiksi testeissä on havaittu monia haavoittuvuuksia SNMPv1 Trap-viestien ja Request-komentojen käsittelyssä. Haavoittuvuudet SNMP-viestien koodin purkamisessa ja sitä seuraavassa prosessoinnissa sekä hallinnointiohjelmien että agenttien puolella voivat johtaa mm. palvelunestohyökkäyksiin ja tahallaan aiheutettuihin puskurin ylivuotovirheisiin (palvelunestohyökkäykset). Jotkut haavoittuvuudet johtuivat siitä, että SNMP-agentti ei vaadi SNMP-viestiltä validia Community Stringiä. Ongelmien johdosta noin 250 yritystä joutui tekemään korjauksia tuotteisiinsa helmikuussa 2002 ja sen jälkeen. (Carnegie Mellon 2002: CERT CA-2002-03)

Perussääntönä SNMP-protokollaa käytettäessä voidaankin pitää sitä, että SNMPv1 ja SNMPv2-protokollia tulisi käyttää vain monitorointiin. Vasta SNMPv3:n avulla voi hallinnointi olla riittävän turvallista konfiguraatiotoimenpiteisiin.

3.1.2 CMIP

Common Management Information Protocol (CMIP) on OSI-mallipohjainen verkonhallintaprotokolla, joka tukee informaationvaihtoa hallintasovellusten ja elementtien välillä. CMIP:n piti valmistuessaan syrjäyttää väliaikainen ja puutteellinen SNMP, ja protokollan kehitys olikin hallitusten ja yhtiöiden rahoitta-

maa. Tavoitteena oli parantaa verkonhallintajärjestelmien toimintamahdollisuuksia. (Carnegie Mellon 2005: CMIP)

CMIP on hyvin perusteellisesti suunniteltu protokolla, joka määrittelee kuinka verkonhallintatietoa vaihdetaan hallintasovellusten ja hallinta-agenttien välillä. Protokolla käyttää ISO:n luotettavaa ja yhteydellistä kuljetusmekanismia ja sisäänrakennettu turvajärjestelmä mahdollistaa autentikoinnin ja turvalogit. (Carnegie Mellon 2005: CMIP)

CMOT (CMIP Over TCP) on TCP/IP-verkoissa toimiva versio CMIP:stä. IEEE 802 –verkoissa käytetään CMOL:ia (CMIP Over LLC).

CMIP:n suurimmat edut verrattuna SNMPv1:een ovat:

- CMIP-muuttujat eivät vain välitä tietoa, vaan niitä voidaan käyttää suorittamaan tehtäviä.
- CMIP on turvallisempi ja se tukee autentikointia, pääsynvalvontaa ja turvalogeja.
- CMIP tarjoaa verkonhallintasovelluksille hyvät mahdollisuudet suorittaa enemmän yhdellä viestillä.
- Paremmat raportit epätavallisista verkkotiloista.

CMIP:iä käytetään varsin laajasti telekommunikaatiopuolella ja laitteet tyypillisesti tukevat CMIP-protokollaa. International Telecommunication Union (ITU) on standardoinut protokollan käytettäväksi telekommunikaatio-laitteiden hallinnassa. (Carnegie Mellon 2005: CMIP)

CMIP on suunniteltu käytettäväksi ISO:n protokollapinossa. Nykyverkot kuitenkin ovat TCP/IP-verkkoja ja useimmat verkkolaitteet tukevat vain SNMP:tä. Vain ani harvat laitteet tukevat CMOT:ia. CMIP kuluttaa myös monimutkaisuudessaan paljon resursseja. Monimutkaisen protokollan päälle on myös vaikeaa ohjelmoida sovelluksia. CMIP-pohjaisen verkonhallintajärjestelmän ylläpitoon voidaan tarvita erikoisosaajia. (Carnegie Mellon 2005: CMIP)

3.2 Järjestelmäratkaisut

Verkonhallintajärjestelmiä on sekä ilmaisia, avoimeen lähdekoodiin perustuvia projekteja, että kaupallisia ratkaisuja, joiden hinnat ulottuvat tuhansiin euroihin. Mitkään näistä eivät ole huonoja, kaikilla on arvonsa, kun niitä käytetään oikein.

Järjestelmän valinnassa oleellisinta on harkita, mitä verkonhallintajärjestelmältä haluaa ja tarvitsee, sekä huomioida verkkoympäristön mahdollisesti asettamat rajoitteet. Oikea valinta riippuu järjestelmän funktiosta, hinnasta ja käyttäjien tarpeista. Ei kannata maksaa täyttä hintaa kalliista kokonaisratkaisusta, jos sen ominaisuuksista käytetään vain 10%.

3.2.1 Microsoft Operations Manager 2005

MOM 2005 on Windows-palvelinten ja -palveluiden valvontajärjestelmä. Sen avulla voidaan keskitetysti kerätä koko organisaation palvelimista tapahtumatietoa, virheilmoituksia ja suorituskykytietoa. MOM valvoo haluttuja palvelimia ja palveluita, sekä ilmoittaa ylläpidolle mahdollisista ongelmista esim. sähköpostilla tai SMS-viesteinä. MOM tallettaa tiedot Microsoft Windows SQL –tietokantaan. MOM:n valvontaan voidaan tuoda myös tunnettujen laitevalmistajien palvelimia (esim. Fujitsu-Siemens, HP ja Dell). Ohjelmistoa voi käyttää vain Microsoft Windows Server -palvelimella. (Microsoft Operations Manager 2006)

Windows-verkoissa MOM:n selkeä etu muihin ovat sen Active Directory –ominaisuudet. Sillä voidaan valvoa syvemmällä tasolla Windows-domainia ja verkon ohjauspalvelinta (Domain Controller) kuin muilla verkonhallintaohjelmistoilla. Näin MOM voi tarjota paljon kattavampaa informaatiota ongelman luonteesta, jos käyttäjä ei esimerkiksi pääse kirjautumaan domainiin. Toisaalta MOM ei ole yhtä universaali kuin muut verkonhallintaohjelmistot. Se soveltuu hyvin Windows-verkkojen ja -palvelinten valvontaan, mihin se on suunniteltu. Muussa käytössä MOM ei anna rahalle täyttä vastinetta.

MOM 2005 -lisenssi hankitaan keskuspalvelimelle sekä lisäksi erilliset Operations Management -lisenssit hankitaan jokaiselle tarvittavalle palvelimelle, joka on MOM serverin hallinnassa. Lisenssin joutuu uusimaan joka toinen vuosi.

Uusi Operations Manager 2007 on kehitysasteella ja julkaistaan lähiaikoina. MOM-kursseja on luonnollisesti tarjolla Suomessakin, jos tarvitsee koulutusta käyttöönottoon ja ylläpitoon.

3.2.2 Nagios

Nagios on avoimeen lähdekoodiin perustuva työasemien, verkkolaitteiden ja palveluiden seurantaohjelmisto, jonka tehtävä on ilmoittaa ongelmista ennen kuin käyttäjät tai asiakkaat niin tekevät. Nagios on suunniteltu käytettäväksi Linux-ympäristössä, mutta se toimii myös useimmissa Unix-varianteissa (esim. FreeBSD, OpenBSD, Sun Solaris, SunOS, IBM AIX, HP-UX). (Nagios 2006: About Nagios)

Nagios ajaa jaksoittaisia tarkistuksia laitteille ja palveluille käyttäen ulkoisia plugineja eli liitännäisiä. Kun ongelmia ilmenee, järjestelmä voi lähettää ilmoituksia ylläpidolle monin eri tavoin (sähköposti, tekstiviesti, IM, jne). Ajantasaisiin tilatietoihin, logeihin ja raportteihin pääsee käsiksi selaimella.

Ominaisuudet:

- Verkkopalveluiden monitorointi (SMTP, POP3, http, NNTP, PING, jne).
- Resurssien monitorointi (suorittimen kuorma, levy- ja muistitilat, prosessit, logit, jne).
- Ympäristöllisten tekijöiden monitorointi (esim. lämpötila).
- Omien tarkistusskriptien käyttömahdollisuus liitännäisinä.
- Verkkolaitehierarkian (status map) määrittelymahdollisuus, jolla voi erottaa toimimattomat laitteet niistä, joihin ei saada yhteyttä.
- Erilaisten ja eritasoisten vikailmoitusten lajittelu kontaktiryhmittäin.
- Mahdollisuus käyttää useita Nagios-palvelimia verkonhallinnan hajauttamiseksi ja varmentamiseksi.
- Monitorointi- ja ilmoitusasetusten muuttaminen www-käyttöliittymästä, tapahtumakäsittelijästä tai kolmannen osapuolen ohjelmilla.
- Tilannetiedon säilyttäminen ohjelman uudelleenkäynnistyksissä.
- Huoltokatkosten määrittely turhien hälytysten välttämiseksi.
- Mm. verkon tila, hälytys- ja ongelmahistoriat, logit www-käyttöliittymässä.
- Käyttäjien oikeuksien määrittely, eri käyttöoikeustasot.
- Ilmainen.

Liitännäisiin perustuvan rakenteen ansiosta Nagiokseen voidaan tehdä minkälaisia tarkistusskriptejä tahansa, aina tarpeen vaatiessa. Lisäksi valmiita liitännäisiä löytyy verkosta varsin runsaasti. Tämä ominaisuus laajentaa valvontamahdollisuuksia huomattavasti sellaisiin laitteisiin ja palveluihin, joita ei monilla muilla verkonhallintajärjestelmillä voida valvoa.

3.2.3 OpenNMS

OpenNMS on ensimmäinen avoimen koodin yrityskäyttöön suunniteltu verkonhallintajärjestelmä. Kaupallisesti OpenNMS:n kehitystä tukee The OpenNMS Group, jonka kautta on saatavilla kaupallisia palveluita, koulutusta ja tukea. Projektilla on runsaasti kehittäjiä. (OpenNMS 2006)

OpenNMS:n tavoitteena on vastata koko ISO:n FCAPS-verkonhallintamalliin. Tärkeimmät OpenNMS:n tehtävät ovat kuitenkin palveluiden seuranta ja raportointi, tiedon keruu, sekä hälytysjärjestelmä. OpenNMS soveltuu hyvin linux- ja unix-pohjaisten palvelinten seurantaan, sekä verkon aktiivilaitteiden hallintaan (esim. Cisco, HP, Jupiter). (OpenNMS 2006)

OpenNMS on pääosin ohjelmoitu Javalla, jotta se olisi mahdollisimman käyttöjärjestelmävapaa. Teoriassa sitä voidaan käyttää missä tahansa järjestelmässä joka tukee Java 1.4 SDK:ta. Valmiiksi käännettyjä ja ajantasaisia ohjelmistopaketteja on saatavilla monelle Linux-distribuutiolle, Solaris 8:lle ja Solaris 9:lle, sekä Mac OS X:lle. Windows-paketit ovat tulossa 2.0 version myötä. (OpenNMS 2006)

OpenNMS:n ominaisuuksiin kuuluu mm.

- Auto Discovery, jolla NMS 24 tunnin välein selvittää onko verkkoon liitetty uusia laitteita.
- Capabilities Daemon, capsd, jolla uusien laitteiden palvelut selvitetään ja lisätään tietokantaan.
- Poller-alijärjestelmä, joka tekee tarkistuksia kaikkiin havaittuihin verkon palveluihin.
- Adaptive polling (mukautuvat kyselyt), kyselyiden väliä tihennetään jos ilmenee ongelma ja esimerkiksi viiden minuutin jälkeen tarkistukset harvenevat ja 12 tunnin kuluttua poistetaan palvelu kokonaan tarkistettavien listalta.
- End User Interface, web-pohjainen käyttöliittymä, josta näkee palveluiden senhetkisen tilan, sekä voi suorittaa erilaisia konfigurointitoimenpiteitä järjestelmään. Suojattu käyttäjänimi- ja salasanayhdistelmällä.
- Passive Status Keeper, joka mahdollistaa palveluiden seurannan passiivisilta laitteilta (laite johon ei saada suoraa yhteyttä).
- SNMPv3 tuki.

Pääasiallinen ero toiseen avoimen lähdekoodin projektiin Nagiokseen on se, että OpenNMS:ää on alusta asti kehitetty yritysten vaatimuksiin järjestelmäksi, jolla on mahdollista monitoroida teoriassa rajatonta määrää laitteita. OpenNMS:ää käytetään jopa kymmenien tuhansien laitteiden monitorointiin. Siksi OpenNMS kilpaileekin enemmän suuren kaupallisen HP OpenViewin kanssa.

OpenNMS on luonnollisesti ilmainen asentaa ja käyttää. Valmiit toimitukset ja tukipalvelut maksavat tuhansia euroja, tapauksesta riippuen.

3.2.4 HP OpenView

OpenView on HP:n Management Software –perheeseen kuuluva kaupallinen verkonhallintajärjestelmä, joka on perinteisesti ollut maailmassa eniten käytetty. HP:n mukaan noin 135000 verkkoa hallinnoidaan OpenViewillä, mm. 67% Yhdysvaltojen palveluntarjoajista käyttää sitä ja kymmenestä suurimmasta jokainen. HP ilmoittaa myös, että noin 70% kaikista maailman verkkolaitteista on OpenViewillä hallinnoituja. (HP OpenView 2006)

OpenViewin ominaisuuksiin kuuluvat mm:

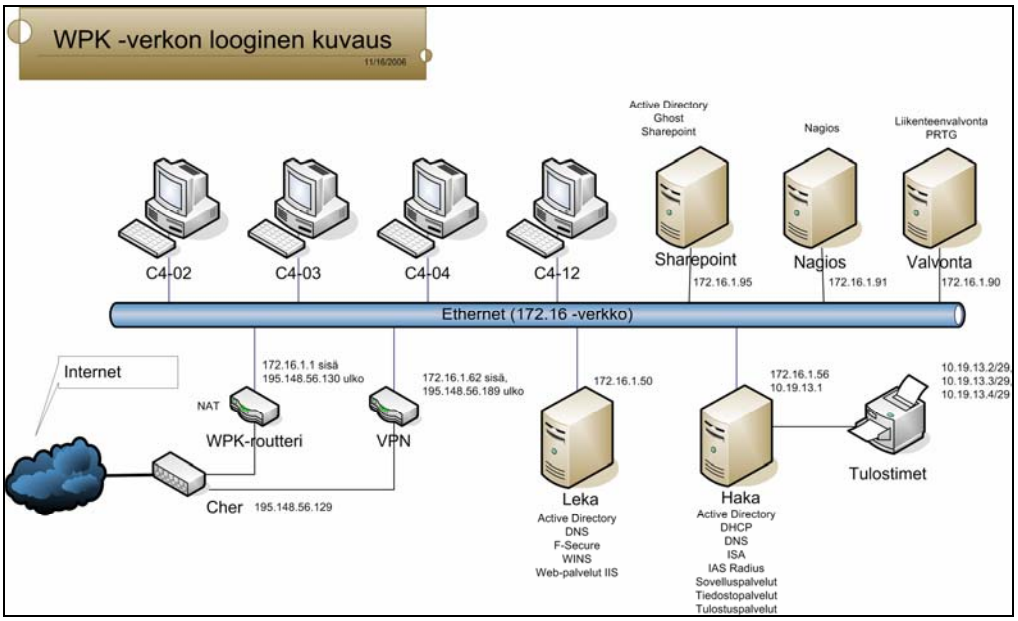
- Graafiset näkymät verkosta ja sen rakenteesta.
- *Automated device discovery and layout*, verkkolaitteiden automaattinen havaitseminen. Löytää TCP/IP, IPX ja kerroksen 2 laitteet (esim. kytkin).
- *Proactive management through reporting and data warehousing*, ongelmakohtien tunnistaminen ja niistä ilmoittaminen ennaltaehkäisevästi.
- *Event correlation technology* osoittaa verkko-ongelmien syyt ja antaa ylläpitäjän nähdä kaikki tapahtumat jotka johtivat hälytykseen. Tarjoaa myös tietoa verkko-ongelmista, jotka aiheuttavat havaittujen kaltaisia oireita.
- Skaalautuvuus.

OpenView Network Node Managerin hankinta kannattaa kilpailuttaa, mutta puhutaan kuitenkin tuhansista tai jopa kymmenistä tuhansista euroista, jos pakettiin lisätään esimerkiksi vuoden päivityssopimus. Lisenssiä itseään ei tarvitse uusia määräajoin, mutta päivityslisenssit ovat maksullisia.

4 Case: WPK-verkko

WPK-verkko on TAMK:n tietoverkkopalveluiden suuntautumisvaihtoehdon tutkimus- ja kehitysverkko, joka on erillinen muusta TAMK:n verkosta ja on tietoverkkopalveluiden omassa hallinnassa. Verkkoon kuuluu n. 100 työasemaa, 50 reititintä, 40 kytkintä ja kuusi palvelinta. Verkon sisäinen nopeus sekä linkki TAMK:n verkkoon on 100 Mbit/s. Käyttäjiä verkolla on n. 100, riippuen kurssien määrästä ja laajuudesta. Kytkimistä ja reitittimistä suurin osa on opetuskäytössä kursseilla, eivätkä ne ole normaalisti osana WPK-verkkoa. Verkko käsittää kolme luokkatilaa ja yhden työhuoneen, jota kutsutaan tutkimus- ja kehityslaboratorioksi. Sinne on sijoitettu myös palvelinhylly, jossa esimerkiksi verkon palvelimet ja WPK-routteri sijaitsevat. Verkkoa ylläpitää ja kehittää täysipäiväisesti yksi harjoittelija sekä muutamat opettajat oman työnsä ohella. Myös TAMK:n tietokonekeskus tarjoaa tukipalveluja tarvittaessa.

Kuvassa 4 on esiteltynä WPK-verkon rakenne. Verkossa käytetään harmaan sarjan ip-osoitteita julkisten säästämiseksi. Työasemat saavat ip-osoitteensa, nimipalvelin- ja yhdyskäytäväosoitteet DHCP-palvelimelta (Haka). Verkko kytkeytyy ulkomaailmaan WPK-reitittimen kautta, joka myös suorittaa osoitteenmuunnoksen. Osa opettajista ja verkon ylläpitäjät pääsevät verkkoon myös salatun yhteyden eli VPN-tunnelin kautta. VPN-liikenne ei ole palomuurilla rajoitettua, eli sillä voidaan käyttää esimerkiksi etätyöpöytää tai muita palveluita, joihin ei normaalisti ulkopuolelta pääse käsiksi. Verkon ohjauspalvelimet (domain controller) ovat Haka, Leka ja Sharepoint. Tulostimet on sijoitettu fyysisesti samaan, mutta loogisesti eri verkkoon, johon pääsee vain tulostuspalvelimen (Haka) kautta. Verkon liikennemääriä tarkkailee Valvonta-kone. Verkon palveluja käsitellään tarkemmin seuraavassa alaluvussa.



Kuva 4: WPK-verkon looginen kuvaus

4.1 Verkon kriittiset toiminnot

Valvonnan piiriin otettiin kaikki verkon kuusi palvelinta ja WPK-verkon reunareititin, joka yhdistää verkon TAMK:n kautta Funettiin. Jokaisella palvelimella on omat roolinsa verkon palveluiden tarjoamisessa. Tässä luvussa käydään läpi kriittiset palvelut ja myöhemmin luvussa 4.5 kerrotaan kuinka näitä palveluita valvotaan.

Toimialueen (domain) ohjauspalvelimen rooli on replikoitu kolmelle palvelimelle, jotka ovat Haka, Leka ja Sharepoint. Näin ollen jos yksikin näistä palvelimista toimii asianmukaisesti, käyttäjä kykenee kirjautumaan työasemalle ja käyttämään sitä. Ohjauspalvelimet välittävät tietoja keskenään jatkuvasti. Verkonhallintapalvelimen tehtävänä on varmistaa, että kaikki kolme palvelinta toimivat asianmukaisesti kaiken aikaa.

DNS-nimipalveluita tarjoaa kaksi palvelinta, Haka ja Leka. Ilman niitä url-osoitteet (esimerkiksi www.google.fi) eivät käänny ip-osoitteiksi ja haluttuun osoitteeseen ei saada luotua yhteyttä. Verkko toimii tällaisessa tilanteessa vain vaivoin. Verkonhallintapalvelin suorittaa kummallekin palvelimelle säännöllisin väliajoin dns-kyselyitä ja näin varmistaa nimipalveluiden toimivuuden.

WPK-verkon DHCP-palvelin on Haka. DHCP (Dynamic Host Configuration Protocol) on protokolla, jonka tehtävänä on jakaa verkkoon kytkeytyville laitteille ip-osoitteet, aliverkkomaski, yhdyskäytävän ja nimipalvelinten osoitteet. Jos DHCP-palvelin ei toimi, työasema ei pääse liikennöimään verkossa ilman että sille asetettaisiin nämä asetukset manuaalisesti.

Hakalla on myös sähköpostipalvelimen rooli. WPK-verkoon ei tule ulkopuolelta sähköpostia, koska opiskelijat ja henkilökunta käyttävät TAMK:n sähköpostiosoitteita. Haka voi kuitenkin lähettää sähköpostia ja esimerkiksi Sharepoint-sivusto käyttää Hakaa lähtevän sähköpostin SMTP-palvelimena.

Verkon web-palvelimia ovat Leka ja Sharepoint. Molemmat käyttävät Microsoftin IIS (Internet Information Services) ohjelmistoa. Lekalla sijaitsevat koulutusohjelman nettisivut ja kurssien opiskelumateriaalit. Sharepoint on portaalipalvelin, jossa on sivustoja eri käyttäjäryhmille. Sharepointille pääsee vain domainin käyttäjätunnuksilla, jos käyttäjällä on oikeudet käyttää ko. sivustoa. Tällä hetkellä sitä käyttävät lähinnä opettajat ja ylläpito keskinäiseen yhteydenpitoon. Tarkoituksena on laajentaa Sharepointin roolia myös oppilaskäytössä, esimerkiksi kurssitehtävien palautuspaikkana.

Leka toimii myös F-Secure Policy Manager -palvelimena, jonka tehtävänä on keskitetysti kontrolloida työasemien F-Secure Internet Security 2006 –ohjelmiston asetuksia ja päivityksiä. F-Securesta ollaan siirtymässä Pandan tuotteisiin.

VPN-palvelin (Virtual Private Network) yhdistää etätyöaseman salatulla yhteydellä eli niin sanotulla VPN-tunnelilla WPK-verkkoon. VPN toimii omana reitittimenään ja sen kautta tuleva liikenne ei kulje WPK-reitittimen kautta. VPN:ää voidaan käyttää esimerkiksi palvelinten etähallintaan tai työasemien etäkäyttöön verkon ulkopuolelta.

WPK-reitittimen rooleihin kuuluvat liikenteen välittämisen lisäksi verkko-osoitteen muunnos eli NAT, sekä nimipalvelut verkon ulkopuolelle. Ilman nattia ei liikenne kulje verkosta ulos eikä sisään. Nimipalvelun rooli taas on mainostaa web-palvelinten, Lekan ja Sharepointin osoitetta ulkomaailmaan.

Tämän lisäksi palvelimiin kuuluu Valvomo-kone, joka seuraa ja tilastoi WPK-verkon liikennettä ja liikennemääriä. Se keskustelee SNMP:n välityksellä verkon reitittimen kanssa.

4.2 Verkonhallintaohjelmisto

TAMK:n tietokonekeskuksella ei ole lisenssiä Microsoft Operations Manager 2005 -ohjelmistoon, joten seuraava laskelma on suuntaa-antava. Lähtökustannus oppilaitoksille tarkoitetulle lisenssille olisi noin 690 euroa hallintaohjelmistosta ja viiden palvelimen valvontalisenssille noin 275 euroa/kpl. Kokonaisuudessaan hallintajärjestelmä kustantaisi noin 85 euroa kuukaudessa Academy-lisensseillä. HP:n raskas OpenView ei tule kysymykseen, koska se olisi myös varsin hintava aloituskustannuksiltaan ja tämän lisäksi suunniteltu käytettäväksi varsin suurissa, tuhansien laitteiden verkossa. Toki sitä voidaan pienemmissäkin käyttää, mutta kustannus on liian suuri ollakseen perusteltavissa järkiperustein. Nagios ja OpenNMS eivät maksa mitään.

OpenNMS on suunniteltu pääasiassa suurten verkkojen hallinnointiin ja on hieman työläämpi asentaa ja ylläpitää kuin Nagios. Lisäksi OpenNMS:ää varten tulisi asentaa PostgreSQL-tietokanta. Tulevaisuuden ylläpitoa ajatellen Nagios on paras vaihtoehto. Se soveltuu hyvin pienten ja keskisuurten yritysten tarpeisiin verkoissa, joissa on kohtuullinen määrä hallinnoitavia laitteita. Näin ollen se on myös soveltuvin käytettäväksi WPK-verkossa.

Nagioksen asennus tehdään manuaalisesti, koska pakettiarkistojen valmiiksi käännetyt versiot eivät ole uusimpia mahdollisia. Manuaalisesta asennuksesta on myös se hyvä puoli, että järjestelmää voidaan päivittää ilman, että Nagios päivittyisi aina muiden yhteydessä. Näin vältytään uudelleenkonfiguroinneilta aina kun niitä ei haluta mahdollisen ohjelmiston päivittämisen vuoksi joutua tekemään. Lisäksi itse käännettäessä saa asennuksesta juuri sellaisen kuin haluaa ja myös käsitys järjestelmän rakenteesta ja toiminnasta on parempi.

Nagioksen ja muiden osien asennusta käsitellään vain hyvin lyhyesti, koska ohjelmien lähdekoodien kääntämiseen ja asentamiseen löytyy hyviä ohjeita verkosta.

4.3 Palvelin ja käyttöjärjestelmä

Verkonhallintajärjestelmää varten koottu palvelinkone on Intel Pentium 4-tasoinen tavallinen työpöytäkäyttöön tarkoitettu keskusyksikkö. Laitteessa on 768 Mt muistia ja kahden gigahertsin prosessori, joka riittää hyvin hallintaohjelmiston ja käyttöjärjestelmän pyörittämiseen. Lisäksi laitteeseen on liitetty Nokia 6310i matkapuhelin datakaapelilla tekstiviestihälytyksiä varten.

Laite on sijoitettu tutkimuslaboratorion palvelinhyllyyn, jossa sijaitsee myös suurin osa valvottavista laitteista. Palvelinta on tarkoitus käyttää etänä joko ssh:n, etätyöpöydän tai selaimen avulla. Perusasennus on tehty paikallisesti, jonka jälkeen laite on asetettu hyllyyn ja konfiguroitu VPN-tunnelin läpi talon ulkopuolelta edellämainituin keinoin.

Palvelimeen ei ole suoraa pääsyä ulkomaailmasta turvallisuussyistä ja siksi, että TAMK:n ulkoisen palomuurin portin avaaminen koettiin hyötyyn nähden liian monimutkaiseksi toimenpiteeksi (kirjallinen hakemus perusteluineen, esimiesten puolto jne). Palvelin itsessään saa vapaasti liikennöidä ulospäin verkkoon, josta esimerkiksi päivitykset noudetaan säännöllisin väliajoin.

Käyttöjärjestelmänä toimii Debian-pohjainen linux-käyttöjärjestelmä Ubuntu Linux Server-versiona. Valintaan vaikuttivat omat kokemukset Debianin erinomaisuudesta palvelinkäytössä sekä Ubuntun valmiudet työpöytäkäytössä, etätyöpöytäyhteyttä ajatellen. Ubuntu käyttää Debianin paketinhallintaohjelmistoa, joka tekee valmiiksi käännettyjen ohjelmien asennuksesta ja päivityksestä helppoa.

4.3.1 Nagioksen asennus

Nagioksen prosessin ajamista varten pitää luoda oma käyttäjä, aivan kuten esimerkiksi www-palvelimellakin linux-ympäristössä. Tämä johtuu siitä, että pääkäyttäjän root-oikeuksin ei tietoturvasyistä kannata ajaa mitään. Kun käytetään normaalia käyttäjätiliä, saadaan sille muokattua yksilölliset oikeudet.

Ennen Nagioksen asentamista on järjestelmään asennettu mm. web-palvelin Apache, PHP, gdlibrary (Graphics Generator Tool) ja monenlaisia kirjastoja Nagiosta varten, jotka helpoiten tähän palvelimeen saa asennettua komennolla *apt-get build-dep nagios*. Lisäksi pitää olla luonnollisesti asennettuna C-kääntäjä (gcc) ja muita kääntämisessä käytettäviä kirjastoja, jotta lähdekoodista saadaan ajettava ohjelma. Koska asennamme kuitenkin uudempaa Nagios 2.5:sta emmekä ykkössarjan versiota, voi jotain puutteita silti jäädä edellämainittujen kirjastojen asennusten jälkeenkin (*apt-get build-dep nagios* tarkistaa vanhemman Nagios 1.3-version riippuvuudet). Ongelmia ei kuitenkaan tästä koitunut. Perusasetusten teon jälkeen voidaan kääntää ja asentaa Nagios. Jos virheitä ei tule, pitäisi Nagioksen olla käyttövalmis, paitsi että ilman liitännäisiä Nagios on käyttökelvoton. Ensin kuitenkin asennetaan web-käyttöliittymä.

4.3.2 Web-käyttöliittymän asennus

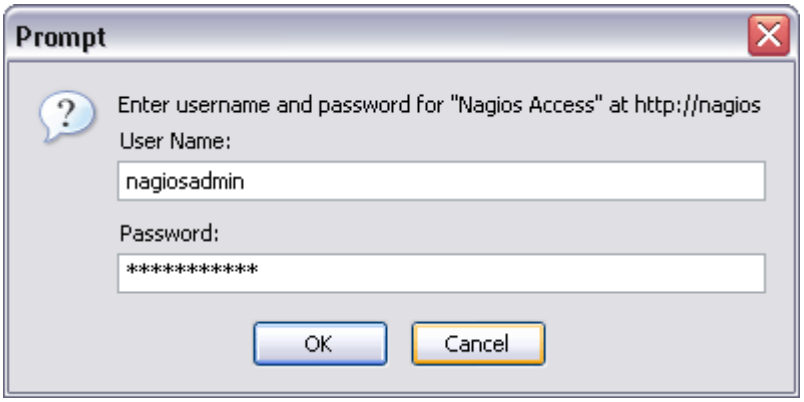
Kun Nagios on asennettu, pitää konfiguroida web-käyttöliittymä ja käyttäjiä, joilla on oikeus käyttää sitä. Nagioksen web-käyttöliittymä suojataan Apachen .htaccessilla, jolla voidaan suojata kokonaisia www-hakemistoja ja tehdä muita sivukohtaisia asetuksia. Käyttäjät ja salasanat generoidaan Apache2:n mukana tulevalla *htpasswd2*-komennolla, esimerkiksi näin:

```
htpasswd2 -nb kayttaja salasana >>
/usr/local/nagios/etc/htpasswd.users
```

Apachen konfiguraatioista pitää sen lisäksi määritellä Nagioksen web-sivujen hakemisto ja vaatia autentikointia sille (require valid-user). AuthUserFile viittaa edellämainittuun htpasswd-tiedostoon, jossa käyttäjät ja näiden kryptatut salasanat ovat. Myös cgi-hakemisto tulee konfiguraatioissa määrittää. Alla esimerkkikonfiguraatio, joka on /etc/apache2/sites-enabled/nagios hakemistossa:

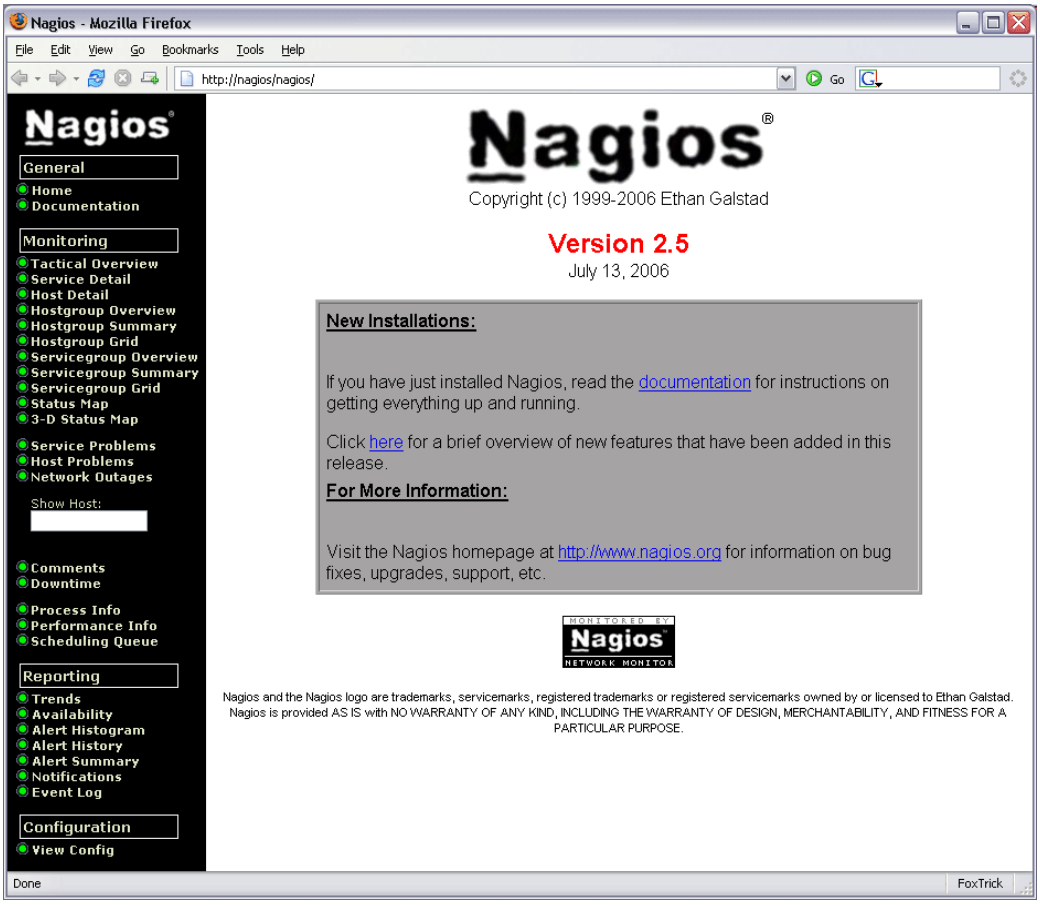
```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<DirectoryMatch /usr/local/nagios/sbin>
            Options ExecCGI
            AllowOverride AuthConfig
            Order Allow,Deny
            Allow From All
            AuthName "Nagios Access"
            AuthType Basic
            AuthUserFile /usr/local/nagios/etc/htpasswd.users
            require valid-user
</DirectoryMatch>

Alias /nagios/stylesheets /usr/local/nagios/share/stylesheets

Alias /nagios /usr/local/nagios/share
<DirectoryMatch /usr/local/nagios/share>
            Options FollowSymLinks
            AllowOverride AuthConfig
            Order Allow,Deny
            Allow From All
            AuthName "Nagios Access"
            AuthType Basic
            AuthUserFile /usr/local/nagios/etc/htpasswd.users
            require valid-user
</DirectoryMatch>
```

Kun asetukset on tehty, käynnistetään Nagios sekä Apache2 uudelleen, jonka jälkeen voidaan koittaa selaimella toimivatko sivut ja autentikointi. Nagios käynnistyy mallikonfiguraatioilla, kunhan konfiguraatiotiedostojen syntaksi on kunnossa.



Kuva 5: Apachen htaccess-autentikointitarkistus

Jos Apachen puolelta on kaikki konfiguroitu oikein, tulisi Nagioksen sivuille pyrkiessä Apachen kysyä käyttäjänimeä ja salasanaa (kuva 5). Kun ne on annettu, aukeaa Nagioksen etusivu (kuva 6).



Kuva 6: Nagioksen web-käyttöliittymän etusivu

Nagios ja käyttöliittymä on asennettu ja seuraava vaihe on Nagioksen varsinainen konfigurointi ja liitännäisten asentaminen.

4.3.3 Nagioksen konfigurointi

Nagioksessa on monia konfiguraatiotiedostoja, jotka pitää luoda tai editoida mallikonfiguraatiotiedostoista, jotta Nagioksella voisi ruveta monitoroimaan palveluja. Nagioksen konfiguraatiokartta (liite 1) auttaa ymmärtämään eri konfiguraatiotiedostojen välisiä suhteita. Pääkonfiguraatiotiedosto on nagios.cfg, jossa määritellään yleisiä asetuksia, jotka vaikuttavat siihen miten Nagios operoi. Tiedostossa määritellään myös muut konfiguraatiotiedostot.

Eräs tärkeimmistä konfiguraatiotiedostoista on cgi.cfg. CGI on tekniikka, jonka avulla selain voi lähettää dataa palvelimella suoritettavalle ohjelmalle. Nagioksessa on toistakymmentä CGI-komponenttia, jotka toistavat Nagioksen tietoja selainkäyttöliittymään, luovat raportteja, keräävät logia tapahtumista, jne. Esimerkiksi Command CGI:n avulla voidaan ohjata Nagiosta web-käyttöliittymästä käsin. Konfiguraatiotiedostossa määritellään näiden komponenttien asetuksia lähinnä siltä kannalta, että mitä kullakin käyttäjällä on oikeus tehdä ja nähdä (yksilölliset pääsytasot).

Muita oleellisia konfiguraatiotiedostoja ovat:

- hosts.cfg, jossa valvottavien laitteiden tiedot on konfiguroitu
- hostgroups.cfg, jossa laitteet mahdollisesti jaotellaan eri ryhmiin
- contacts.cfg, johon laitetaan niiden henkilöiden yhteystietoja, joille lähetetään hälytyksiä
- services.cfg, jossa määritellään verkon palvelut ja niiden tarkistukset
- checkcommands.cfg, jossa määritellään tarkistuskomennot ja niiden syntaksi
- misccommands.cfg, jossa määritellään esimerkiksi notification-komennot hälytyksiä varten (esim. sähköpostin tai tekstiviestin lähetys)

Käytännössä konfiguraatiotiedostot voisi yhdistää yhdeksi suureksi tiedostoksi, mutta osiin jaoteltuna konfigurointi on helpompaa. Ne voi myös nimetä miten haluaa. Tässä on käytetty oletusnimiä, jotta mahdollisesti asennettavalle konfigurointityökalulle ei koituisi ongelmia löytää konfiguraatiotiedostoja. Liitännäisiin liittyvistä konfiguraatiotiedostoista (mm. services, checkcommands ja hosts) puhutaan lisää seuraavassa luvussa.

Aina konfiguraatioiden muuttamisen jälkeen Nagios on uudelleenkäynnistettävä, jotta muutokset tulevat voimaan. Konfiguraatioiden syntaksin voi myös tarkistaa komennolla */usr/local/nagios/bin/nagios –v konfiguraatiotiedosto.cfg*.

4.3.4 Liitännäiset ja niiden konfigurointi

Liitännäisiä (plugins) käytetään tarkistusten tekemiseen ja Nagioksen pluginspaketti asennetaan samalla tavalla kuin Nagioskin, kääntämällä lähdekoodista. Liitännäisiä voi asentaa niin paljon kuin haluaa ja tehdä itsekin. Suurin osa Nagioksen liitännäisistä on ohjelmoitu Perl-kielellä. Nagioksen oma kokoelma

on kohtuullisen kattava, ja perusasioiden seurantaan se riittää. Näihin kuuluvat esimerkiksi mm. DHCP, DNS, SMTP, FTP, SSH, POP ja Telnet.

Ylimääräisiä, verkosta haettuja ja asennettuja lisäliitännäisiä olivat

- check_snmp_load, joka selvittää prosessorien käyttöasteet
- check_snmp_storage, joka kertoo massamuistien tilasta
- check_snmp_win, jolla voi tarkistaa palveluiden toiminnan (esim. IIS)
- check_winmem, jolla tarkistetaan muistinkäyttö Windows-palvelimissa

Jotta ymmärrämme vähän paremmin, miten liitännäiset käytännössä toimivat, katsotaan kuinka konfiguraatiot vaikuttavat toisiinsa. Esimerkkinä konfiguroidaan prosessorin käyttöasteet selvittävän liitännäisen ja siihen liittyvien konfiguraatiotiedostojen konfiguraatiot.

Oleellisin asia on tietää liitännäisen syntaksi. Tämän voi selvittää komennolla *./check_snmp_load.pl -h*, missä check_snmp_load.pl on itse liitännäisskripti. Tuloksena saadaan paljon tietoa liitännäisen käytöstä:

```
SNMP Load & CPU Monitor for Nagios version 1.3
(c)2004-2006 Patrick Proy

Usage: ./check_snmp_load.pl [-v] -H <host> -C <snmp_community>
[-2] | (-l login -x passwd [-X pass -L <authp>,<privp>]) [-p
<port>] -w <warn level> -c <crit level>
-T=[stand|netsl|netsc|as400|cisco|cata|nsc|fg|bc|nokia|hp|lp]
[-f] [-t <timeout>] [-V]
-v, --verbose
print extra debugging information
-h, --help
print this help message
-H, --hostname=HOST
name or IP address of host to check
-C, --community=COMMUNITY NAME
community name for the host's SNMP agent (implies v1 protocol)
-2, --v2c
Use snmp v2c
-l, --login=LOGIN ; -x, --passwd=PASSWD
Login and auth password for snmpv3 authentication
If no priv password exists, implies AuthNoPriv
-X, --privpass=PASSWD
Priv password for snmpv3 (AuthPriv protocol)
-L, --protocols=<authproto>,<privproto>
<authproto> : Authentication protocol (md5|sha : default md5)
<privproto> : Priv protocole (des|aes : default des)
-P, --port=PORT
SNMP port (Default 161)
-w, --warn=INTEGER | INT,INT,INT
1 value check : warning level for cpu in percent (on one min-
ute)
3 value check : comma separated level for load or cpu for
1min, 5min, 15min
-c, --crit=INTEGER | INT,INT,INT
critical level for cpu in percent (on one minute)
1 value check : critical level for cpu in percent (on one min-
```

```
ute)
3 value check : comma separated level for load or cpu for
1min, 5min, 15min
-T, --type=stand|netsl|netsc|as400|cisco|bc|nokia|hp|lp
CPU check :
stand : standard MIBII (works with Windows),
can handle multiple CPU.
netsl : linux load provided by Net SNMP
netsc : cpu usage given by net-snmp (100-idle)
as400 : as400 CPU usage
cisco : Cisco CPU usage
cata : Cisco catalyst CPU usage
nsc : NetScreen CPU usage
fg : Fortigate CPU usage
bc : Bluecoat CPU usage
nokia : Nokia CPU usage
hp : HP procurve switch CPU usage
lp : Linkproof CPU usage
-f, --perfparse
Perfparse compatible output
-t, --timeout=INTEGER
timeout for SNMP in seconds (Default: 5)
-V, --version
prints version number
```

Oikea syntaksi esimerkiksi Haka-palvelimen tarkistamiseen olisi: *./check_snmp_load.pl -H 172.16.1.56 -C n4g10s -2 -w 98 -c 99. -H* määrittää tarkistettavan kohteen osoitteen, *-C* SNMP Community Stringin, *-2* SNMPv2-protokollan, *-w* varoitustason ja *-c* kriittisen tason (prosentteina). Tarkistuksen voi ajaa itse manuaalisesti ja varmistaa, että vastauksena saadaan todellista tilannetta vastaava arvo. Tässä tapauksessa vastauksena saadaan ”2 CPU, average load 3.5 < 98 : OK”. Tarkistus toimii ja se voidaan asettaa Nagioksen konfiguraatioihin.

Liitännäistä käyttävä komento konfiguroidaan Nagioksen checkcommands.cfg -tiedostoon. Luodaan komento c*heck_snmp_load* ja lisätään sille komennon syntaksi:

```
# 'check_snmp_load' command definition
define command{
            command_name      check_snmp_load
            command_line      $USER1$/check_snmp_load.pl -H
            $HOSTADDRESS$ -C $ARG1$ -$ARG2 -w $ARG3$ -c $ARG4$
}
```

Kaikki testaamisessa käytetyt muuttujien arvot korvataan makroilla, jotka Nagios korvaa asianmukaisilla arvoilla tarkistusta ajettaessa. Tämä tehdään siksi, että komento olisi universaali. Sillä voidaan valvoa kymmeniä eri laitteita. $HOSTADDRESS$ korvataan laitteen osoitteella ja $ARG1$ Community Stringillä. Muut arvot olivat käytettävän SNMP-version, varoitustason ja kriittisen tason määrittelyjä. $USER1$ viittaa hakemistoon, joka on Nagioksen

konfiguraatiossa määritetty liitännäisten asennuspaikaksi, mistä ne myös löytyvät.

Kun komento itsessään on konfiguroitu, määritellään sen tarkistamat laitteet services.cfg-tiedostossa. Laitteiden lisäksi annetaan tarkistuksen aikana korvattavien makrojen arvot.

```
# CPU LOAD SNMP
define service{
            use                 generic-service
            host_name           SHAREPOINT,HAKA,LEKA
            service_description      CPU LOAD
            check_period        24x7
            contact_groups      admins
            …
            check_command       check_snmp_load!n4g10s!2!98!99
}
```

Host_name määrittelee laitteet, joille tarkistuksia lähetetään. Kuten esimerkissä, voidaan yhdessä määritelmässä luetella monta laitetta jolle tarkistuksia lähetetään. Jos halutaan käyttää eri parametreja eri laitteille, voidaan tehdä toinen vastaava palvelukuvaus, johon määritellään eri laitteet ja parametrit. Laitteiden asetukset on määritelty erikseen hosts.cfg-tiedostossa, joten tässä viitataan vain laitteiden nimiin. Tarkistuksia ajetaan ympäri vuorokauden (24x7) ja mahdollisen ongelman sattuessa ilmoituksia lähetetään admins-ryhmän henkilöille (konfiguroitu contactgroups.cfg ja contacts.cfg –tiedostoissa). *Check_command* viittaa checkcommands.cfg:ssä aiemmin määriteltyyn komentoon *check_cnmp_load*, ja sille määritellään lähetettäväksi neljä lisäoptiota, jotka olivat SNMP Community String (n4g10s), käytettävä SNMP-versio (2), varoitustaso (98) ja kriittinen taso (99).

Hälytyksiä Nagios lähettää joko varoitustasolla, kriittisellä tasolla tai molemmilla riippuen siitä, miten hälytykset on konfiguroitu.

Jos ilmenee, että Nagioksella on ongelmia suorittaa komentoa, johtuu se useimmiten siitä, että käyttäjä on unohtanut asettaa Nagios-käyttäjälle oikeudet ajaa tarkistusskriptiä.

4.3.5 NRPE

NRPE (Nagios Remote Plugin Executor) on Nagioksen taustaprosessi valvottaville palvelimille. Sitä käytetään sellaisten asioiden valvomiseen joita ei voi suoraan etänä selvittää. Tällaisessa tapauksessa NRPE tekee tarkistuksia paikallisesti palvelimella ja on yhteydessä Nagiokseen. NRPE voidaan asentaa myös Windows-palvelimille.

Jos valvottavia laitteita on paljon, tulisi selvittää saako SNMP:llä selville ne asiat, joita NRPE:llä suunnittelee valvovansa. Usein esimerkiksi levytiloja, muistin käyttöä tai muita vastaavia asioita valvotaan NRPE:llä, vaikka SNMP-kysely suoriutuisi samasta tehtävästä niin, ettei jokaiselle palvelimelle tarvitsisi asentaa NRPE-taustaprosessia. Palvelimilla ei kannata pyörittää mitään ylimääräistä. Tämä on oleellinen asia sekä resurssien riittävyyden, että tietoturvan kannalta.

Edellämainituista syistä NRPE ei ole käytössä WPK-verkossa, eikä sen asentamista sen vuoksi tässä käsitellä. NRPE:n sijaan käytetään SNMP-kyselyitä.

4.3.6 NSCA

Nagios Service Check Acceptor on Nagioksen lisäosa, jota käytetään tarkistustietojen välittämiseen Nagios-palvelimelta toiselle. Aktiiviset tarkistukset ovat palvelimen itsensä tekemiä, passiiviset tarkistukset ovat toisen Nagios-palvelimen lähettämiä tarkistustuloksia, jotka NSCA ottaa vastaan.

NSCA voi tulla kyseeseen, kun halutaan replikoida verkonhallinta useammalle palvelimelle varmuuden vuoksi, tai kun halutaan jakaa kyselykuormaa kahdella tai useammalla palvelimella. WPK-verkossa NSCA ei ole käytössä, koska verkkoa hallinnoidaan yhdellä palvelimella.

4.4 SMS-hälytysjärjestelmä

Esimerkiksi Siemens valmistaa tekstiviestihälytyslaitteita, jotka on suunniteltu tämänkaltaisiin käyttötarkoituksiin. Koska laitteet ovat kalliita, hoidettiin hälytysjärjestelmän rakentaminen WPK-verkossa hyvin maanläheisesti vanhahkolla Nokia 6310i –kännykällä, joka liitettiin datakaapelilla palvelinkoneeseen. Verkonhallintajärjestelmä käyttää Gnokiita kriittisten hälytysten lähettämiseen tekstiviestillä.

Gnokii (GNU-Nokia) on avoimeen lähdekoodiin perustuva projekti, joka tarjoaa työkalut ja ajurit useimpien Nokian matkapuhelinten käyttämiseen Linux-, Unix- ja Win32-käyttöjärjestelmissä. Gnokiin avulla voi esimerkiksi tehdä datapuheluita, päivittää osoite- yms tietoja, käyttää kalenteria, lähettää ja vastaanottaa tekstiviestejä ja ladata soittoääniä puhelimeen (Gnokii 2006: About Gnokii).

Itse Gnokiin konfigurointiin ei tässä perehdytä sen enempää. Nagioksessa komennot tekstiviestien lähettämiseen on konfiguroitu misccommands.cfg-tiedostossa. Komennon syntaksi on seuraava:

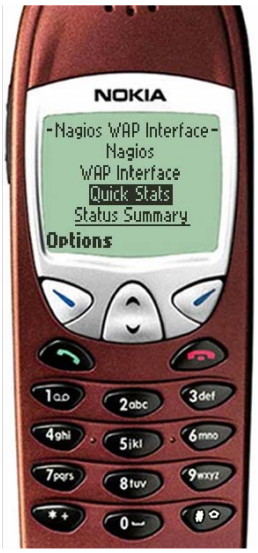
```
# 'notify-by-gnokii' command definition
define command{
            command_name      notify_by_gnokii
            command_line
            /usr/local/nagios/bin/sms_notification_by_gnokii
            $CONTACTPAGER$ "$NOTIFICATIONTYPE$ alert -
            $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$ -
            $SERVICEOUTPUT$"
}
```

Suurin osa komennosta on siis makroja, jotka korvataan komentoa suorittaessa määritellyillä muuttujanarvoilla sekä hälytykseen tulevalla tiedolla ongelmasta. Sms_notification_by_gnokii on itse asiassa lyhyt shell-skripti joka käyttää gnokiita viestin lähettämiseen. Skriptin syntaksi on seuraavanlainen:

```
#!/bin/sh
#sms_notification_by_gnokii.pl
#
mess=$2
number=$1
echo $mess | gnokii --sendsms $number
```

Nagios-käyttäjällä tulee olla oikeus käyttää skriptiä sekä sitä palvelimen porttia, johon puhelin on liitetty. Tässä tapauksessa portti on ensimmäinen sarjaportti (/dev/ttyS0). Muuten Gnokii ei suostu lähettämään komentoja puhelimelle.

Mobiilitoiminnot voidaan myös laajentaa kaksisuuntaisiksi siten, että Nagiosta voidaan käyttää matkapuhelimen datayhteydellä mistä tahansa (kuva 7). WPK-verkossa tätä ominaisuutta ei otettu käyttöön.



Kuva 7: Nagioksen WAP-käyttöliittymä (Nagios: Screenshots)

4.5 Valvonta käytännössä

Verkon valvottavat palvelut vielä lyhyesti sanottuna olivat:

- DNS (Haka, Leka, WPK-ROUTTERI)
- DHCP (Haka)
- SMTP (Haka, Nagios)
- HTTP (Leka, Nagios)
- Sharepoint (Sharepoint)
- SSH (Nagios)

Lisäksi järjestelmä katsoo, että jokainen laite vastaa yhteydenottoihin eli toimii perustasolla. Tämän lisäksi valvotaan fyysisiä ominaisuuksia kuten levytilaa, prosessorikuormitusta ja muistinkäyttöä.

Valvottavan kohteen tila on joko OK, WARNING tai CRITICAL. OK se on silloin, kun palvelu vastaa halutusti tai vastauksena saatu arvo (esimerkiksi käytetty levytila) on alle määritellyn WARNING-tason, esimerkiksi 80%. Kohteen tilaksi tulee CRITICAL, jos palvelu ei vastaa uudelleentarkistuksienkaan jälkeen, tai jos vastauksena saatu arvo on yli kriittiseksi määritellyn tason. Hälytykset voi konfiguroida haluamallaan tavalla. WPK-verkossa pääperiaate on se, että vain kriittisten palveluiden kriittiset ilmoitukset saavat aikaan tekstiviestihälytyksiä. Sähköpostihälytyksiä järjestelmä lähettää jo WARNING-tasolla.

DNS-palveluita valvotaan niin, että Nagios tekee jatkuvasti nimikyselyitä kullekin palvelimelle. Jos pyyntöön ei vastata kolmella perättäisellä yrityskerralla, merkitsee Nagios palvelun tilaksi CRITICAL ja lähettää hälytyksiä, jos ne ovat päällä.

Verkon osoitetietojen jakamista valvotaan tekemällä DHCP-kyselyitä samalla varmistaen, että niihin vastaa oikea palvelin (Haka). Toinen, verkkoon kuulumaton DHCP-palvelin sotkisi verkko-osoitteiden jakelun ja näin ollen koko verkon liikenteen. Verkkopalveluiden kursseilla näinkin voi vahingossa käydä.

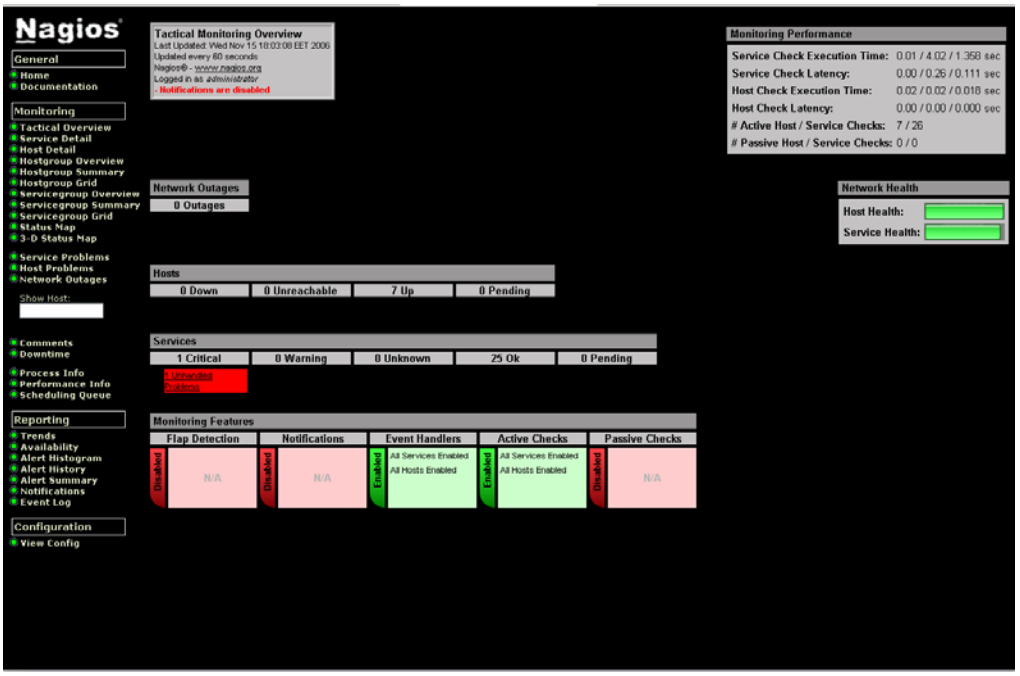
Myös Hakan sähköpostipalvelua valvotaan suorin kyselyin ja katsotaan, että se vastaa asianmukaisesti. Jotta Nagioksen lähettämät sähköpostihälytykset eivät kuitenkaan olisi Hakan toiminnasta riippuvaisia, käyttää verkonhallintapalvelin omaa SMTP-prosessiaan sähköpostin lähettämiseen. Lisäksi se myös valvoo sitä. Nagios ei vastaa ulkoa tuleviin SMTP-pyyntöihin. Lekan ja Nagioksen www-palvelimia valvotaan samalla periaatteella, http-kyselyillä.

Sharepoint on ensimmäinen listan palveluista, jota ei valvota suoraan käyttämällä ko. palvelua. Yksi vaihtoehto olisi ollut sellaisen liitännäisen asentaminen, joka osaa autentikoitua palvelimelle käyttöoikeustarkistuksen yhteydessä. Päätin kuitenkin valvoa prosessia SNMP-liitännäisen avulla. Tämä liitännäinen tarkistaa, että Sharepoint-prosessi on käynnissä palvelimella. Samalla tavalla

voitaisiin valvoa mitä tahansa palvelimella pyörivää prosessia. Myös levytiloja, muistinkäyttöä ja prosessorien käyttöasteita valvotaan SNMP:llä.

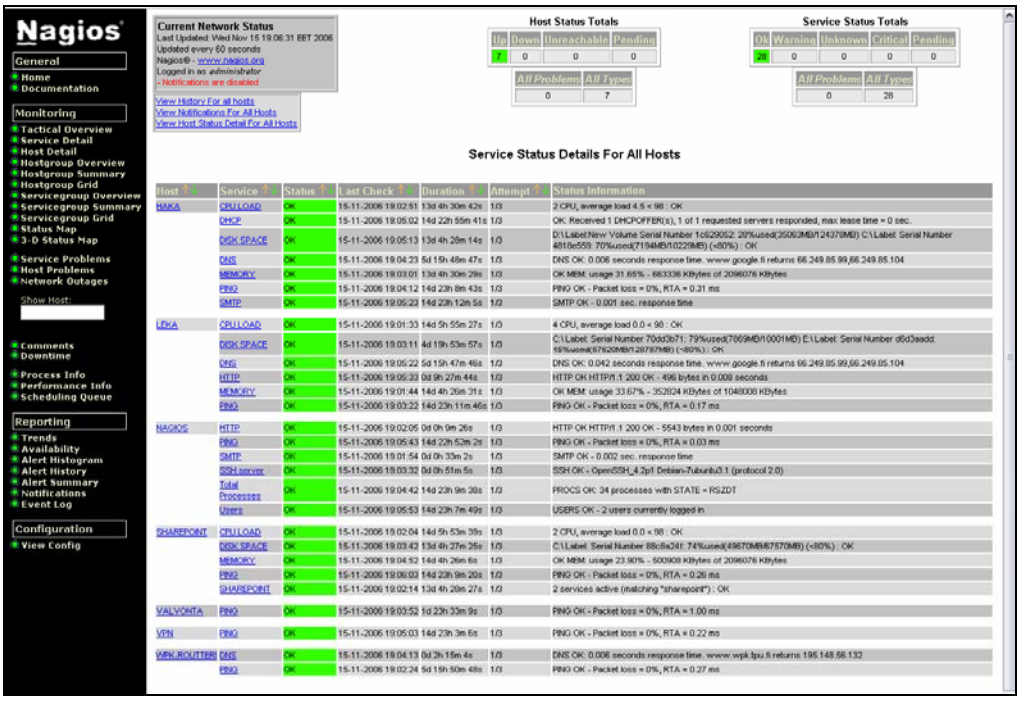
Lekan F-Secure Policy Manager -palvelua ei valvota, koska F-Securesta ollaan siirtymässä lähiaikoina Pandan antivirus- ja palomuuriohjelmistoihin.

Luonnollisesti Nagios lähettää ilmoituksia, jos joissain näistä palveluista ilmenee ongelmia. Verkon tilaa voi myös seurata Nagioksen web-käyttöliittymästä. Tactical overview -sivu (kuva 8) kertoo jo oleellisimman verkon tilasta, eli ovatko hälytykset päällä, toimivatko palvelimet ja kaikki palvelut.



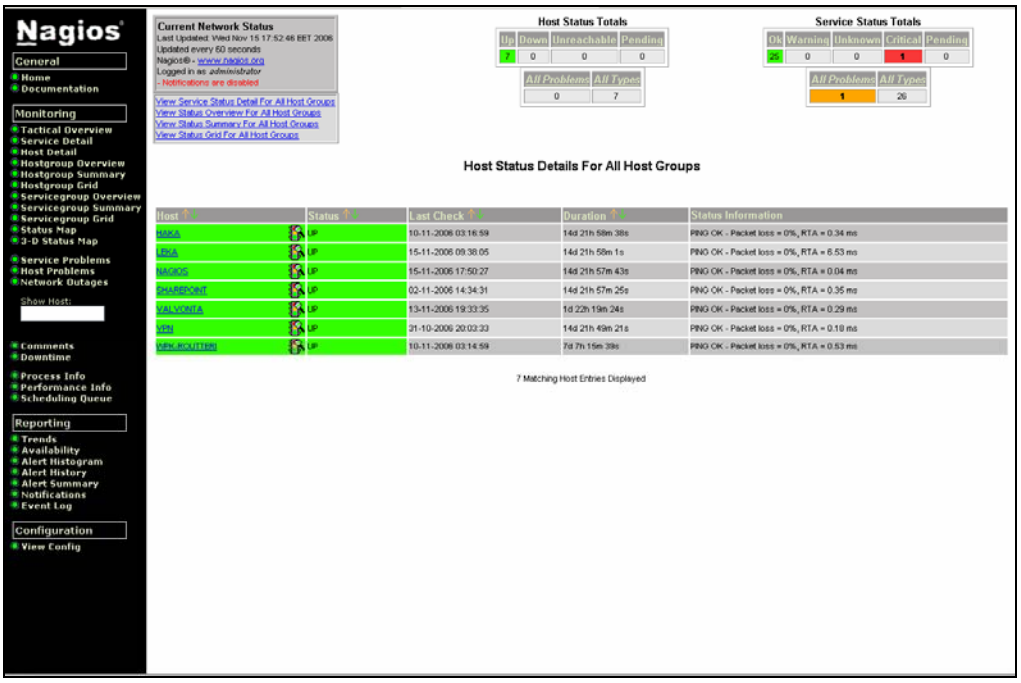
Kuva 8: Nagios - Tactical Overview

Service detail -sivu (kuva 9) on kaikkein informatiivisin. Siltä näkee suoraan kaikkien valvottujen palveluiden tilanteen ja myöskin lisätietoja niiden tilasta. Kun kaikki toimii, on palveluiden tila OK ja väri vihreä. Varoitustilassa olevat palvelut näkyvät listassa keltaisella ja kriittiset punaisella, joten niitä on vaikeaa olla huomaamatta.



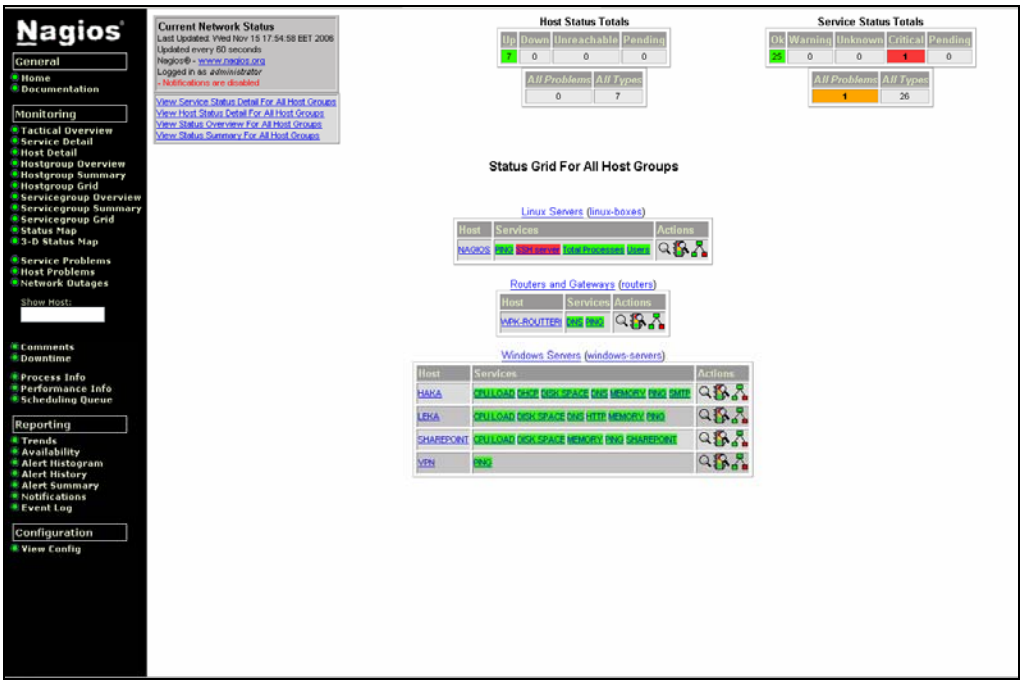
Kuva 9: Nagios – Service Detail

Host detail -sivulta (kuva 10) voi katsoa, ovatko kaikki laitteet toiminnassa. Tältä sivulta saa tiedon vain siihen, onko laite ylipäätään siinä kunnossa että se pystyy ottamaan vastaan ns. ping-paketin ja lähettämään siihen vastauksen. Vaikka laite olisikin kunnossa, voivat yhteysongelmat aiheuttaa sen, että laite näkyy punaisena Nagioksessa. Toisaalta palvelimen tarjoamien palveluiden kannalta on aivan sama, onko laite tavoittamattomissa vai jollakin tavalla rikki, kyseiset palvelut ovat joka tapauksessa menetettyjä toistaiseksi.



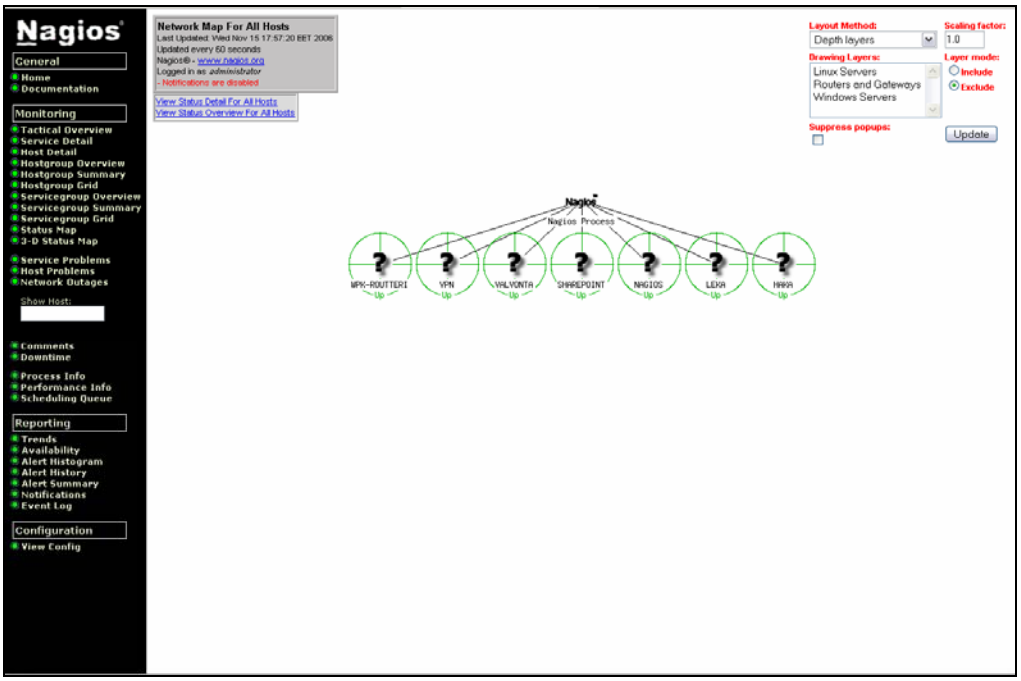
Kuva 10: Nagios – Host Detail

Hostgroup-sivut summary, overview ja grid (kuva 11) tarjoavat periaatteessa kaikki samat tiedot valvottavista laitteista ja näiden palveluista. Näillä sivuilla palvelimet ja palvelut on jaoteltu palvelin- ja laiteryhmittäin, joka on hyödyllistä varsinkin kun valvottavana on useita kymmeniä tai jopa satoja laitteita. Myös palvelut voidaan jakaa ryhmiin ja niitä voidaan tarkastella samalla periaatteella.



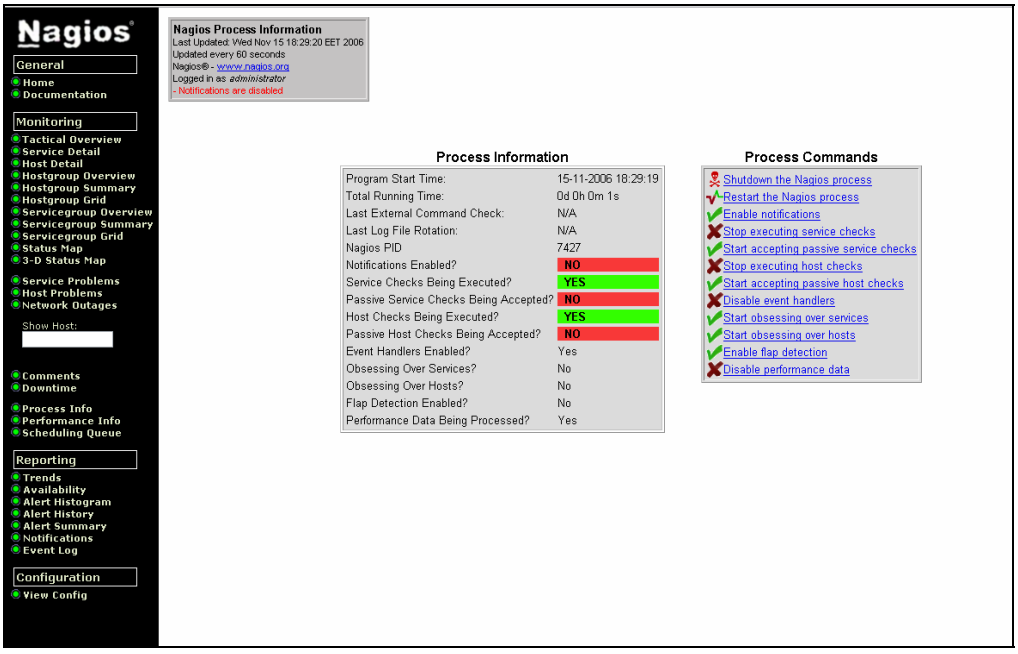
Kuva 11: Nagios – Hostgroup Grid

Status map on graafinen kuva verkosta (kuva 12). Siihen voidaan konfiguroida riippuvuussuhteita ja verkkoja siten, että esimerkiksi nähdään mikä segmentti verkosta on tavoittamattomissa. WPK-verkon tapauksessa tällaista tarvetta segmentointiin ei ole.



Kuva 12: Nagios – Status Map

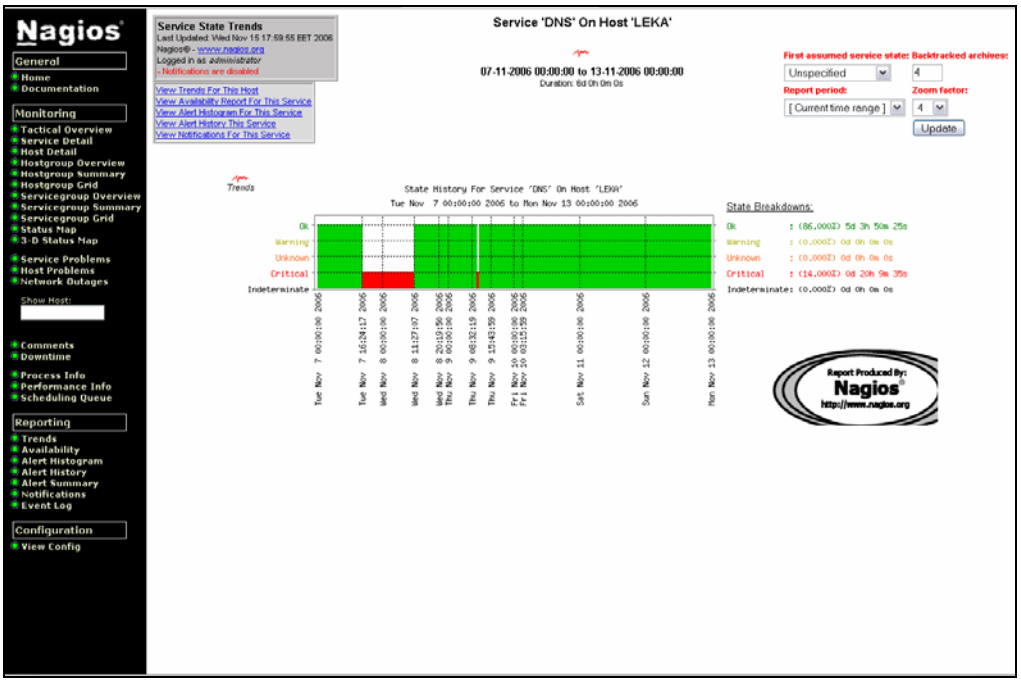
Process info (kuva 13) on ylläpidolliselta kannalta oleellinen sivu, koska sieltä näkee joitain yleisiä asetuksia ja niitä voi myös muuttaa samasta paikasta. Lisäksi tältä sivulta Nagioksen voi sammuttaa tai uudelleenkäynnistää, sekä suorittaa muita komentoja, mikäli käyttäjällä on niihin oikeudet.



Kuva 13: Nagios – Process Info

Trends-työkalulla voidaan laatia raportteja ja kuvaajia eri laitteiden ja niiden palveluiden toiminnasta. Esimerkkikuvassa (kuva 14) näkyy Lekan DNS-

palvelun toiminta valittuna ajankohtana sekä toimivuusongelmat, joiden syynä oli WPK-reitittimen hajoaminen.



Kuva 14: Nagios – Trends

4.6 Turvallisuus

Nagios-palvelinta on mahdollista hallita Nagioksen web-käyttöliittymän lisäksi SSH:lla tai VNC:llä (etätyöpöytä). Kaikissa näissä on käyttäjätunnus/salasanasuojaus, ja salasanat ovat MD5-kryptattuina salasanatiedostoissa. Yleisten sanojen MD5-hashit on jo jossain määrin selvitetty, mutta satunnaisten kirjain- ja numeroyhdistelmien purkamiseen menee niin paljon aikaa, että ne voidaan ainakin tällä hetkellä vielä katsoa murtamattomiksi. Nagios-palvelimeen ei pääse verkon ulkopuolelta käsiksi lainkaan. Ainoastaan VPN-tunnelin kautta palvelinta on mahdollista hallita ulkopuolelta. Tämä estää tehokkaasti ns. brute force -hyökkäykset palvelimelle, joissa syötetään automaattisesti käyttäjätunnus- ja salasanayhdistelmiä tuhatmäärin. Sellaisiin osoitteisiin, joissa SSH-portti on avoin, näitä hyökkäyksiä tulee päivittäin. On kuitenkin erittäin epätodennäköistä, että sisäverkosta kukaan tekisi hyökkäystä palvelimelle. Palvelimella joka tapauksessa on fail2ban-ohjelma, joka estää tällaiset hyökkäykset. Logitiedostoista voidaan myös jälkikäteen selvittää, mistä osoitteista hyökkäyksiä on tullut. Jos palvelimeen pääsisi suoraan SSH:lla ulkopuolelta, voisi SSH-palvelimen myös turvallisuussyistä laittaa kuuntelemaan eri porttia.

Aiemmin käsiteltyihin SNMP:n turvallisuusongelmiin on varauduttu siten, että palvelimet vastaavat SNMP-pyyntöihin vain, jos ne tulevat Nagiokselta. Lisäksi palvelimia ei ole tarkoitus hallita SNMP:n avulla, joten palvelimilla on vain SMNP-lukuoikeudet. Myös Community String on asetettu ja käytössä on

SNMPv2, joka on edes hieman turvallisempi kuin edeltävä versio. Käytössä olevilla Windows Server 2003 –käyttöjärjestelmillä ei ole suoraa SNMPv3-tukea, joka olisi luonnollisesti ollut turvallisin versio.

5 Yhteenveto

Toimeksiannon mukaisesti tämän opinnäytetyön oleellisin tavoite oli järjestää tietoverkkopalveluiden koulutusohjelman verkon palvelinten hallinnointi. Tähän tarkoitukseen asennettu Nagios-verkonhallintaohjelmisto oli soveltuvin ja myös edullisin tämän päämäärän saavuttamiseksi. Nagioksen vahvuus WPK-verkossa on myös se, että liitännäisiin perustuvan toteutuksensa ansiosta se soveltuu hyvin monenlaisten laitteiden ja alustojen hallintaan. Tutkimus- ja kehitysverkkona WPK-verkkoon saatetaan tuoda monenlaisia komponentteja tulevaisuudessa, jolloin Nagios mitä todennäköisimmin taipuu myös näiden laitteiden valvontaan oikealla liitännäisellä.

Työssä esittelin verkonhallintaa, verkonhallintajärjestelmiä ja verkonhallinnan standardoituja protokollia, erityisesti SNMP:n ongelmia. Käytännön osiossa ei niinkään keskitytty Nagioksen ja muiden komponenttien asentamiseen, koska niihin löytyy oppaita, esimerkiksi Nagioksen omat dokumentaatiot. Käytännön osion päähuomio oli verkon palveluissa, niiden valvonnan järjestämisessä ja Nagioksen roolissa näiden tehtävien suorittajana.

Nykyisen verkon ja sen laitteiden valvonta Nagioksella tulee hoidettua vähintäänkin riittävästi. Jokainen kriittinen palvelu on tarkassa seurannassa ja ongelmista lähtee vikailmoituksia. Erityisesti SMS-hälytysjärjestelmän käyttöönottomahdollisuus vaikutti ilahduttavan myös toimeksiantajaa ja puhelin tähän tarkoitukseen saatiin hankittua melko nopeasti. Ylläpitoa järjestelmä auttaa myös siten, että voidaan yhdellä silmäyksellä todeta verkon toiminnallinen tila.

Ohjelmistona Nagios on vakaa, eikä se ole oikutellut monen kuukauden käytön yhteydessä kertaakaan. Kaikki ongelmat, joita Nagioksen kanssa on koettu, ovat johtuneet käyttäjästä.

Järjestelmän ongelmakohtana voidaan pitää sitä, että asiaan perehtymättömälle Nagioksen asentaminen ja jopa ylläpito voi olla ylivoimaisen vaikeaa. Konfiguraatiotiedostoja on paljon ja niiden syntaksin on oltava täysin oikein, muuten Nagios ei käynnisty lainkaan. Nagiosta varten tehdyt konfiguraatiotyökalutkin ovat vain tekstieditoreita toisessa muodossa, eivätkä tuo juuri mitään käytännön helpotusta asetusten muuttamiseen. Jos parempia työkaluja jostain löytyy, sellaisen asentaminen voisi helpottaa järjestelmän konfigurointia jatkossa henkilölle, joka ei entuudestaan tunne järjestelmää. Tämän lisäksi Nagioksessa voisi olla ns. autohunt-ominaisuus, joka löytäisi verkkoon liitetyt uudet laitteet automaattisesti.

Järjestelmän voisi myös laittaa seuraamaan ja tilastoimaan verkon liikennemääriä. Sitä varten on kuitenkin jo verkossa olemassa oma järjestelmänsä, joka on toteutettu PRTG Traffic Grapherilla.

Yleisesti ottaen verkonhallintajärjestelmät vapauttavat paljon resursseja verkon ylläpitäjiltä ja helpottavat ongelmanratkaisua, erityisesti suurissa verkoissa. Niiden avulla saavutetaan parempi toimivuus ja kustannussäästöjä, sekä voi-

daan ennustaa ja perustella paremmin tulevaisuudessa tehtäviä hankintoja. Näistä järjestelmistä Nagios soveltuu hyvin käytettäväksi pienissä ja keskisuurissa verkoissa.

Olen hyvin iloinen siitä, että verkonhallintapalvelin ja hälytysjärjestelmä tulivat käyttöön oikeaan ympäristöön ja aitoon tarpeeseen. Toivon, että palvelin palvelee tarkoitustaan mahdollisimman hyvin, ja että sen potentiaali hyödynnetään myös tulevaisuudessa uusien laitteiden ja palveluiden valvonnassa.

Lähdeluettelo

Drake, Peter 1991. Using SNMP to manage networks. Designing Resilient Architectures, IEE Colloquium 15.11.1991, IEEE.

Leinwand, Allan & Fang Conroy, Karen 1996. Network management – a practical perspective. Addison Wesley Longman, Inc

Stevens, W. Richard 2000. TCP/IP Illustrated, Volume 1. Addison-Wesley.

Carnegie Mellon University, Software Engineering Institute 2002. CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP) [online] [viitattu 14.10.2006] http://www.cert.org/advisories/CA-2002-03.html

Carnegie Mellon University, Software Engineering Institute 2005. Common Management Information Protocol – Software Technology Roadmap [online] [viitattu 22.9.2006].
http://www.sei.cmu.edu/str/descriptions/cmip_body.html

Cisco Systems, 2002. Simple Network Management Protocol. Internetworking Technology Handbook [online] [viitattu 2.8.2006]
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

Gnokii project. [online] [viitattu 10.9.2006]. www.gnokii.org

HP OpenView Management Solutions. [online] [viitattu 20.9.2006].
www.managementsoftware.hp.com

Microsoft Operations Manager. [online] [viitattu 20.10.2006].
www.microsoft.com/mom/

Netstatz Solutions. [online] [viitattu 5.10.2006]. www.netstatz.com/solutions/

Official Nagios website. [online] [viitattu 12.9.2006]. www.nagios.org

OpenNMS network management platform. [online] [viitattu 12.9.2006].
www.opennms.org

SNMP Research International, 2006. SNMPv3 White Paper. [online] [viitattu 22.10.2006] www.snmp.com/snmpv3/v3white.shtml

Liitteet

Liite 1: Nagioksen konfiguraatiokartta